Janne Siltainsuu

KYBERRIKOLLISUUS MODERNISSA TIETOYHTEYSKUNNASSA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2017

TIIVISTELMÄ

Siltainsuu, Janne
Kyberrikollisuus modernissa tietoyhteiskunnassa
Jyväskylä: Jyväskylän yliopisto, 2017
Tietojärjestelmätiede, kandidaatintutkielma, 42 s.
Ohjaaja(t): Koskelainen, Tiina

Tämä tutkielma käsittelee kyberrikollisuutta modernissa tietoyhteiskunnassa. Tutkimuksessa pohditaan kyberrikollisuuden ilmenemistä, kyberrikollisten motiiveja sekä suojautumista kyberrikoksia vastaan. Kyberrikollisuus ilmenee yhteiskunnassa kyberavusteisina rikoksina sekä kyberriippuvaisina rikoksina. Kyberavusteiset rikokset ovat rikoksia, joiden toteuttaminen olisi mahdollista ilman tietoverkkoja. Kyberavusteisissa rikoksissa rikos tapahtuu verkon avulla, mutta se ei ole edellytys. Kyberavusteisia rikoksia ovat mm. sähköisillä markkinapaikoilla tapahtuvat petokset. Kyberriippuvainen rikos on laiton teko, joka vaatii tietoverkon rikoksen tekovälineeksi. Kyberriippuvaisen rikoksen toteuttaminen ilman tietoverkkoja ei ole mahdollista. Kyberriippuvainen rikos on esim. palvelunestohyökkäys, jonka toteuttaminen ilman tietoverkkoja on mahdotonta. Kyberrikolliset voidaan jakaa karkeasti kolmeen luokkaan: ammattirikollisiin, haktivisteihin sekä valtioihin. Ammattirikolliset pyrkivät saavuttamaan rikoksillaan taloudellista hyötyä, haktivistit ajamaan poliittista tai ideologista agendaa ja valtiot pyrkivät ajamaan omaa kansallista etuaan. Kyberrikolliset kehittävät jatkuvasti uusia ansaintamalleja jotka ovat luovia ja helposti kopioitavissa uuteen ympäristöön. Näistä kiristyshaittaohjelmahyökkäykset ovat jatkuvasti ajankohtainen esimerkki. Nykyisin kyberrikoksen uhriksi joutuminen on yleisempää kuin rikoksen uhriksi joutuminen reaalimaailmassa. Kyberrikokselta on siksi tärkeätä suojautua. Yksilöt voivat suojautua tehokkaasti ylläpitämällä tietoturvatietoisuutta, päivitettyjä selaimia ja käyttöjärjestelmiä sekä ottamalla käyttöön asianmukaiset tietoturvaohjelmistot. Organisaatioiden on noudatettava samoja ohjeita kuin yksilöiden, mutta organisaation on pohdittava kyberturvallisuutta laajemmassa kontekstissa. Organisaation on pidettävä huolta henkilökunnan koulutuksesta, sillä henkilöstö on usein helpoin tapa toteuttaa tietomurto. Organisaation on pidettävä huolta jatkuvuussuunnittelusta sekä tietoverkkojen segmentoinnista. Usein puhutaan tietoturvassa olevan ihmisongelmia sekä teknisiä ongelmia. Teknisiin ongelmiin vastaus on jatkuvan tilannekuvan ylläpito ja toimiminen havaittuihin tarpeisiin ja poikkeamiin tilannekuvan perusteella. Ihmisongelmiin vastauksena on säännöllinen ja jatkuva koulutus sekä tietoisuuden kasvattaminen.

Asiasanat: kyberrikos, kyberavusteinen rikos, kyberriippuvainen rikos, kyberrikollinen, tietoturva, kyberturva, tietomurto, haittaohjelma, haktivismi

ABSTRACT

Siltainsuu, Janne
Cybercrime in a modern information society
Jyväskylä: University of Jyväskylä, 2017
Information Systems Science, Bachelor thesis, 42 s.
Supervisor(s): Koskelainen, Tiina

This study looks in to cybercrime in the modern information society. In this study the aim is to examine cyber criminality as phenomena in society, the motives behind the crimes and how an individual or an organization can protect itself from cybercrimes. Cybercrime is seen in two types of crimes in the society. Types are cyber assisted crimes and cyber dependent crimes. Cyber assistant crimes are crimes that can be done without computers or computer networks. They are crimes like cyber assistant fraud in an electronic market place. Cyber dependent crimes are crimes that cannot be done without computers and networks. They are crimes like denial of service attacks. Cyber criminals can be roughly categorized in three groups professional criminals, hactivists and nation states. Professional criminals seek economic income in their crime, hacktivists are seeking attention for their political or ideological agenda and nation states are seeking their own national interests. Cyber criminals are constantly developing new ways to generate income that are creative and can be copied easily in to a new environment. Ransom malware attacks are a recent and common example of this. In the modern society, it is more likely to become a victim of a cybercrime than an actual crime in the real world. This is the reason why everyone should protect themselves from cybercrime. Individual people can protect themselves by improving their cyber security awareness, keeping software updated and implementing necessary security software on their workstations. Organizations need to think the cyber security in a larger view. Organization need to educate the staff about cyber security related matters, since the staff is usually the biggest risk. Organizations need to keep their contingency plans up to date and implement segmentation to their networks. Very often the security is divided in to people problems and technical problems. Technical problems can be handled with situation awareness, but the human problem requires regular training to keep the organization secure.

Keywords: cybercrime, cyber assisted crime, cyber dependent crime, cybercriminal, information security, cyber security, information breach, malware, hacktivism

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tällä hetkellä elämme aikaa, jossa internetistä ja sen tarjoamista palveluista on tullut osa jokapäiväistä elämäämme. Internetistä ja verkon palveluista on tullut omalla tavallaan luontainen ympäristö miljoonille ihmisille (Kritzinger & Von Solms, 2010). Palvelut jotka aiemmin vaativat fyysistä läsnäoloamme voidaan hoitaa nykyisin paikasta tai ajasta riippumattomasti. Internet tarjoaa meille loputtoman tietovaraston, aidosti globaalin markkinapaikan sekä mahdollisuuden kommunikoida koko maailman kanssa ajasta ja paikasta riippumatta. Kuitenkin näiden mahdollisuuksien ja vapauksien myötä kasvavat samassa suhteessa riskit joutua kyberrikoksen uhriksi. Kyber- ja tietoturvallisuus koskettavat tällä hetkellä kaikkia ja vaativat huomiota jokaisella alalla. Laajalle levinneet tietojärjestelmät herättävät myös vihamielisen hyökkääjän mielenkiinnon. (Backhouse & Dhillon, 1996) Kaikkien verkossa toimivien toimijoiden on ensiarvoisen tärkeätä tuntea verkossa toimimisen riskit sekä henkilökohtaisen tiedon turvaamisen periaatteet, jotta voidaan ymmärtää seuraukset turvallisuudelle mikäli tietoja, toimintoja ja prosesseja ei suojata oikein (Kritzinger & Von Solms, 2010).

Kyberrikollisuudesta aiheutuvat kustannukset syntyvät rikosten aiheuttamasta vahingosta yrityksille ja yhteiskunnalle. Kyberrikollisuus aiheuttaa vahinkoa kaupankäyntiin viennissä ja tuonnissa, hidastaa innovointia ja maailmantalouden kasvua. Vuonna 2014 kyberrikollisuuden on arvioitu maksavan maailmanlaajuisesti 0,8 % globaalista bruttokansantuotteesta, jota voidaan verrata vastaavaan arvioon, jonka mukaan huumerikollisuuden saman kaltainen vaikutus on 0,9 %. (McAfee, 2014) Yleisimmät kyberrikokset ovat haittaohjelmien valmistus ja tartuttaminen, verkkohuijaukset sekä tietojen kalastelu. Kyberrikollisuuden todellista määrää on hankala arvioida, sillä vain kaksi kymmenestä rikoksen uhrista tekee rikosilmoituksen (Symantec, 2011.) Kuten kaikissa rikoksissa, myös kyberrikoksissa rikoksen toteutuminen perustuu aina tilaisuuteen, kykyyn toteuttaa rikos sekä motiiviin. Kybertoimintaympäristö voidaan nähdä rajapintana tavanomaiselle rikokselle. (Felson & Clarke, 1998)

Tämä kirjallisuuskatsauksena toteutettu tutkimus tutkii kyberrikollisuuden vaikutusta ja ilmenemistä modernissa tietoyhteiskunnassa. Tutkimuksen tavoit-

teena on selvittää, miten kyberrikollisuus ilmenee modernissa tietoyhteiskunnassa, minkälaisia erilaisia tapoja sekä motiiveja rikollisilla on hyötyä rikoksella sekä miten yksityishenkilö ja organisaatio voivat suojautua kyberrikollisuudelta. Tutkimuksen tavoitteena on myös tuottaa ymmärrystä ja ohjeita yksityishenkilölle sekä organisaatioille kyberrikollisuudesta ja sitä vastaan suojautumisesta. Yksilöt ja organisaatiot voivat suojautua verkkorikollisuutta vastaan noudattamalla hyviä tietoturvakäytäntöjä. Organisaatioiden osalta on kiinnitettävä huomiota teknisten toteutusten lisäksi liiketoimintalogiikkaan, toipumis- ja jatkuvuussuunnitteluun sekä henkilökunnan koulutukseen. Tutkimus on toteutettu käyttämällä avoimien lähteiden lisäksi mahdollisimman kattavasti eri tietoturvaalan toimijoiden julkaisuja, tieteellisiä artikkeleita sekä painettuja teoksia, jotka käsittelevät kyberrikollisuutta sekä tietoturvaa. Lähteiden osalta tutkimuksessa suhtaudutaan kriittisesti ja arvioivasti tietoturvayhtiöiden tuottamaan tietoon, sillä yhtiöiden tunnetaan pyrkivän lisäämään myyntiä suurentelemalla uhkia.

Tutkimuksessa pohditaan vastauksia seuraaviin kolmeen kyberrikollisuutta ja sen vaikutuksia koskeviin kysymyksiin:

- Miten kyberrikollisuus ilmenee modernissa tietoyhteiskunnassa?
- Minkälaisia motiiveja kyberrikollisilla on?
- Miten yksilöt ja organisaatiot voivat suojautua kyberrikollisuutta vastaan?

Tietoturvallisuudella tarkoitetaan tässä tutkimuksessa tietojen, palveluiden ja tietoliikenteen suojaamista, jolla taataan tietojen luottamuksellisuus, eheys ja saatavuus. (Peltomäki & Norppa, 2015)

Modernilla tietoyhteiskunnalla tarkoitetaan yhteiskuntaa, jossa palveluita ja hyödykkeitä välitetään sähköisesti. Modernissa tietoyhteiskunnassa kansalaisilla on pääsy suoraan tai välillisesti tietoverkkoon. Modernissa tietoyhteiskunnassa päivittäisiä palveluita voidaan hoitaa verkon välityksellä. Näitä palveluita tarjotaan etäpalveluina, jolloin hyödykkeitä ja palveluita voidaan tilata internetistä ja ne toimitetaan vastaanottajalle siten, että toimittaja ja ostaja eivät tapaa fyysisesti. Palvelut ja hyödykkeet voivat olla maksullisia tai maksuttomia. (viestintävirasto, 2015) Tällaisia palveluita ovat pankkipalvelut, sosiaalipalvelut, veropalvelut ja muut vastaavat palvelut.

Kriittisellä infrastruktuurilla tarkoitetaan kaikkia yhteiskunnan ylläpitäviä keskeisiä toimintoja kuten energiansiirto ja -jakelu, logistiikka, vesihuolto, raha- ja finanssijärjestelmät sekä sähköiset viestintäjärjestelmät (Valtioneuvoston kanslia, 2010). Kriittinen infrastruktuurimme toimii tietoverkkojen varassa, sillä informaatiota välitetään tietoverkkojen välityksellä eri kriittisen infrastruktuurin järjestelmille (Hoffman, Rosenberg, & Washington, 2005). Kriittinen infrastruktuuri sisältää myös kriittisen informaatioinfrastruktuurin, joka koostuu fyysisistä ja virtuaalisista järjestelmistä. Nämä järjestelmät kontrolloivat, prosessoivat, säilövät ja välittävät digitaalista sisältöä, joka ohjaa kriittistä infrastruktuuria. (Limnéll, Majewski & Salminen, 2014).

Kyberturvallisuudella tarkoitetaan tietoturvan laajempaa käsitettä, joka tarkoittaa tilaa, jossa kybertoimintaympäristöön voidaan luottaa ja sen tarkoituksenmukaisesti toiminnasta voidaan huolehtia. (Peltomäki & Norppa, 2015)

Kyberrikollisuus määritellään yksinkertaisimmillaan rikokseksi, joka toteutetaan tietoverkon avulla (Nykodym ym., 2005). Kyberrikollisuudella tarkoitetaan tässä tutkimuksessa laitonta toimintaa, joka tapahtuu verkossa. Kyberrikolliset pyrkivät hyötymään näistä rikoksista rahallisesti, saavuttamalla maksullista sisältöä ilmaiseksi, keräämällä mainetta tai tiedustelutietoa sekä hankkimalla kuuluvuutta omalla ideologiselle, uskonnolliselle tai poliittiselle näkemykselle.

Kyberavusteinen rikos on lainvastainen teko, jonka toteuttaminen ei vaadi välttämättä tietokoneita tai tietoverkkoja rikoksen toteuttamisessa. Tällaisia rikoksia ovat mm. petokset jotka toteutetaan verkon sähköisillä markkinapaikoilla. Kyberavusteisissa rikoksissa tietoverkko toimii rajapintana rikokselle, mutta ei vaadi sitä rikoksen toteutumisessa.

Kyberriippuvainen rikos on lainvastainen teko, jonka toteuttaminen vaatii tietokoneen ja/tai tietoverkon rikoksen tekovälineeksi ja näiden rikosten toteuttaminen on mahdollista vain tietoteknisessä ympäristössä. Tällaisia rikoksia ovat esimerkiksi tietoverkkorikosvälineen hallussapito, tietomurrot sekä tietoliikenteen häirintä palvelunestohyökkäyksin. (Viestintävirasto, 2016e).

Tietoturvallisuudella tarkoitetaan tässä tutkimuksessa tietojen, palveluiden ja tietoliikenteen suojaamista, jolla taataan tietojen luottamuksellisuus, eheys ja saatavuus. (Peltomäki & Norppa, 2015)

Tutkimuksessa käsitellään aluksi kyberrikolliset sekä kyberrikollisuuden uhrit. Näiden kautta siirrytään käsittelemään rikosta sekä rikoksen toteuttamista eri konteksteissa. Viimeisessä luvussa annetaan ohjeita yksilölle sekä organisaatiolle kyberrikoksen uhriksi joutumisen välttämiseksi.

2 KYBERRIKOLLISUUDEN ILMENEMINEN JA TOIMINTATAVAT MODERNISSA TIETOYHTEISKUNNASSA

Peltomäki ja Norppa (2015) määrittelevät sanan kyber seuraavasti: Kyber-sana tulee kreikan sanasta kybereo, jonka merkitys on ohjata, opastaa ja hallita. Kyber tarkoittaa sähköisessä muodossa olevan informaation käsittelyä. Limnéll, Majewski ja Salminen (2014) määrittelevät sanan kyber seuraavasti: ”kyber on etuliite, jolla viitataan tieto- ja kommunikaatioteknologian mahdollistamaan digitaalisen maailman ilmiöön, tapahtumiin, toimijoihin, toimintoihin, toimintatapoihin ja normeihin.” Kyberrikollisuudelle Limnéll, Majewski ja Salminen (2014) eivät erikseen määrittele yhtä yhteinäistä määritelmää, sillä myöskään lainsäädäntö ei tunne suoraan kyberrikollisuutta tai kyberrikosta. Tämä heijastelee heidän mukaansa ilmiön ja käsitteen moniselitteisyyttä sekä sen tunnuspiirteiden jatkuvaa ja nopeata muutosta. Kyberrikollisuus voidaan kuitenkin määritellä kapea-alaisesti miksi tahansa laittomaksi toiminnoksi, joka kohdistuu tietokoneisiin, digitaaliseen tietoon, tietojärjestelmiin tai- verkkoihin (Limnéll ym., 2014). Suomen poliisi määrittelee kyberrikollisuuden rikoksiksi, jotka kohdistuvat tietoverkkoon tai tietotekniikkaan sekä rikoksiksi, jotka toteutetaan tietotekniikkaa tai tietoverkkoja hyväksi käyttäen (Poliisi, 2016). Kyberrikos voidaan nähdä myös viitekehyksenä jossa toteutuu aina kolme ehtoa. Kyberrikos rikkoo ihmisoikeuksia, rikos on tahaton tai tahallinen teko ja siihen kuuluu suunnittelu ja/tai toteutus, joka on teknologia-avusteinen. (Helfenstein & Saariluoma, 2014) Edellä mainittuja tukee myös määritelmä, jonka mukaan kyberrikos ei välttämättä ole uusi ja innovatiivinen rikostyyli, vaan ennemminkin tapa toteuttaa vanhoja rikoksia uudella tavalla tehokkaammin ja niin, että kiinnijäämisen riski on huomattavasti pienempi. (McCusker, 2006) Tästä voidaan pitää esimerkkinä Bangladeshiläisen pankin ryöstämistä tietoverkosta käsin, jossa kyberrikolliset saivat saaliiksi 81 miljoonaa yhdysvaltojen dollaria. (Hyppönen & Tuominen, 2017)

Kyberrikollisuutta ilmenee nykyisin kaikissa verkottuneissa tietoyhteiskunnissa. Rikollisuus on seurannut normaalia rikoksen polkua siirtymällä sinne, minne myös kuluttaminen, liiketoiminta ja yhteiskunta ovat siirtyneet (Peltomäki & Norppa, 2015). Kyberrikollisuus ei monellakaan tapaa eroa perinteisestä rikollisuudesta, sillä molemmissa pyritään ensin tunnistamaan kohde käyttämällä tarkkailua sekä psykologista profilointia. Kyberrikollisuuden ja perinteisen rikollisuuden välinen ero on Jahankhani ja Al-Nemratin (2016) mukaan siinä, että kyberrikollisen ei tarvitse olla läsnä rikoksen tapahtuessa rikospaikalla, samassa maassa tai edes välttämättä samassa maanosassa.

Nykyisin trendinä on siirtää mahdollisuuksien mukaan kaikki informaation manipulointi sekä hakeminen digitaaliseen muotoon. Informaation digitalisointi ajaa sekä organisaation että yksilön etuja. Sotateorian tohtori Martti Lehto kuvailee verkossa tehtailtavien rikosten olevan kustannustehokasta, sillä kiinnijäämisen riski on pieni, rangaistukset ovat alhaisia tai lainsäädäntö ei kyseisessä maassa tunne rikosta sekä ihmiset ovat liian luottavaisia toimiessaan verkossa

(Peltomäki & Norppa, 2015, s. 34). Näyttääkin siltä, että tällä hetkellä eletään murrosvaihetta jossa teknologia on kehittynyt liian nopeasti, jotta tavallinen kuluttaja pystyisi havainnoimaan riskejä sekä varautumaan niihin. Tällä hetkellä kuluttajat ovat haavoittuvia kyberrikoksille sillä heillä ei ole riittävää tietämystä laitteiden suojaamisesta, tietoturvallisuudesta tai henkilökohtaisen tiedon suojaamisesta verkkopalveluissa (Kritzinger & Von Solms, 2010). Kuluttajien tietämys on tällä hetkellä lastenkengissä, sillä verkossa toimivat palvelut ovat monimutkaisia ja niissä toimiminen on moniulotteista. On arvioita, että verkossa rikoksen uhriksi joutuminen on todennäköisempää kuin rikoksen uhriksi joutuminen reaalimaailmassa (Hintsala, 2016). Tätä tukee myös Symantecin (2011) teettämä tutkimus, jossa kyberrikoksen uhriksi joutumisen todennäköisyydeksi on arvioitu 1/2.27. Tutkimuksen mukaan kyberrikoksen uhrit joutuvat todennäköisemmin myös muiden rikosten uhriksi. Kyberrikollisuus on tehokas tapa toimia, sillä se mahdollistaa suorien resurssien ja informaation jakamisen rikollisyhteisössä, jonka avulla voidaan maksimoida operationaalinen tehokkuus, joustavuus sekä toiminnan nopea vaste (Jahankhani & Al-Nemrat, 2016).

2.1 Kyberrikolliset

Tavanomaiset rikolliset määritellään viiteen eri kategoriaan rikollisten motiivien ja toimintatavan mukaan. Tavanomaisia rikollistyyppejä ovat huvittelijat (recreational), tilaisuuteen tarttujat (occasional), osittain ammattilaiset (occupational), ammattilaiset (professional) ja ideologiset (ideological). (Hagan, 2010) Rikoksia huvikseen tehtailevat henkilöt toteuttavat rikoksia ilman suurempaa motiivia. Heidän tavoitteensa on tehdä rikoksia huvikseen ja siksi koska he pystyvät siihen. Huvikseen rikoksia tehtailevien motiiveihin ei yleensä kuulu taloudellisia motiiveja. Tilaisuuteen tarttujat tarttuvat tilaisuuteen, jossa jokin toiminto tai virhe on jättänyt tilanteen haavoittuvaiseksi rikokselle. Osittain ammatikseen rikoksia tekevät henkilöt tekevät rikoksia usein, mutta he eivät kuitenkaan tee niitä saavuttaakseen siitä koko elinkeinoa. Osittain ammattilaisten motiivit ovat käytännössä aina taloudellisia. Ammattirikolliset tekevät rikoksia saavuttaakseen sillä taloudellista etuutta. Ammattirikollisten motiivit ovat käytännössä aina välillisesti tai välittömästi taloudelliset. Ideologiset rikolliset eivät pyri saavuttamaan taloudellista etua vaan tekevät rikoksia ajaakseen jotain poliittista, uskonnollista tai muuten aatteellista tarkoitusperää. Ideologisten rikosten taustalla on harvoin taloudellisia perusteita. Taloudelliset perusteet ideologisissa rikoksissa liittyvät yleensä rikoksen kohteena olevan tappioiden kasvattamiseen eivätkä omien tulojen maksimoimiseen. (Hagan, 2010)

Peltomäki ja Norppa (2015) jakavat kyberrikolliset kuuteen eri ryhmään osaamisen ja motiivin perusteella. Kyberrikolliset jaotellaan tietämättömiin, hakkereihin, haktivisteihin, ammattirikollisiin sekä valtiollisiin toimijoihin. Samantyylistä luokittelua käyttää Kevin Taylor (2005), jossa kyberrikolliset on luokiteltu samaan tyyliin kuuteen eri ryhmään, muuleihin (mule), ammattilaisiin (professionals), valtiollisiin toimijoihin (nation state actors), aktivisteihin (activists),

sisäpiiriin kuuluviin henkilöihin (insider) ja nuorisoon (gateway). Tietoturvavaikuttaja Mikko Hyppönen (2012) jakaa kyberrikolliset kolmeen joukkoon: haktivistit, rikolliset sekä valtiot. Yhtenäistä kaikille näille on niiden jako tehdään selkeästi ideologisen ja taloudellisen hyötymisen välille. Erona luokitteluilla on, että Hyppönen (2012) ei jaottele tarkemmin rikollisten sisällä toimijoita pienempiin lokeroihin.

Tietämättömillä rikollisilla tarkoitetaan sellaisia henkilöitä, jotka osallistuvat kyberrikoksen toteuttamiseen tietämättään tai toimivat hyvässä uskossa. Henkilö voi tietämättään ladata saastuneen ohjelman tietokoneelleen tai älylaitteeseen, jonka kautta laite voidaan kaapata ja sitä voidaan käyttää hyödyksi kyberrikoksen toteuttamisessa (Peltomäki & Norppa, 2015). Hyvässä uskossa toimivia henkilöitä käytetään mm. rahamuuleina. Taylor (2012) kuvaileekin tietämättömiä vastaavaa ryhmää muuleina (mules) omassa luokittelussaan. Tällaiset rikolliset ottavat vastaan rikoksena saatuja hyödykkeitä ja osallistuvat tietämättään tai tietoisesti mm. rahanpesuun sekä varastetun tavaran välittämiseen (Taylor, 2005). Molemmissa kuvauksissa rahamuulilla tarkoitetaan henkilöä, joka palkataan toimimaan rahanvälittäjänä ja hänen työnsä on käsitellä transaktioita. On mahdollista, että tällaiset henkilöt eivät itse tiedä olevansa rikoksessa mukana, sillä he ovat usein henkilöitä, jotka etsivät helppoja, kotoa käsin tehtäviä etätöitä. Kyberrikolliset palkkaava useita muuleja, jolloin operaatioista tulee vaikeampia selvittää. Lähi-idässä toteutetussa väärennettyjä pankkikortteja hyväksikäytetyssä rikoksessa arvioidaan toimineen 500 muulia, joiden palkkaus perustui 5 - 10% provisioon. (McAfee, 2014) Tietämättömien motiivit vaikuttavat olevan taloudelliset, kuvaukseen liittyy tavalla tai toisella rahallinen hyötyminen. Tietämättömät hyötyvät rikoksillaan kuitenkin taloudellisesta näkökulmasta melko vähäisesti, joten tietämättömiä voidaan pitää osittain ammattimaisina rikollisina.

Välinpitämättömien ryhmällä tarkoitetaan henkilöitä, jotka eivät miellä välttämättä toimintaansa rikokseksi tai pitävät sitä vähäisenä. (Peltomäki & Norppa, 2015) Taylor (2005) luokittelee tällaiset rikokset nuorisoksi (gateway). Tällaiset henkilöt käyttävät usein internetistä saatavilla olevia valmiita työkaluja eivätkä osallistu itse niiden kehittämiseen. Henkilöt ovat usein nuoria ja heitä ei yleensä uhkaa kovinkaan kova vankeusrangaistus. Usein nuoria rikollisia leimaa myös tarve näyttää muille omia kykyjään. Tällaisia rikoksia ovat vertaisverkosta laittoman sisällön lataaminen kuten musiikki, elokuvat tai ohjelmistot. Oikeuspoliittisen tutkimuslaitoksen (2012) tekemän tutkimuksen mukaan 15 – 16 vuotiaista 79% ilmoitti ladanneensa elämänsä aikana laitonta sisältöä vertaisverkoista ja 71% ilmoitti tehneensä niin kuluneen 12 kuukauden sisällä (Salmi, 2012). Vertaisverkoilla tarkoitetaan tiedonsiirtorakennetta, jossa käyttäjät välittävät tiedostoja tai tietoja toisilleen käyttämättä mitään keskitettyä välityspalvelinta. Välinpitämättömät vaikuttavat olevan toimintatavoillaan tilaisuuteen tarttujien kaltaisia. Tähän on viitteitä siitä, että hyödykkeiden saatavuuden parantamisella on pystytty vähentämään tietoverkoissa tapahtuvaa piratismia, jolloin on henkilöt ovat alkaneet maksaa kuluttamastaan sisällöstä. (Das, 2000) Välinpitämättömät

voivat kuulua myös ideologisten rikollisten luokkaan, sillä heidän välinpitämättömyytensä saattaa johtua ideologisesta pohjasta, jolloin toiminta on heidän mielestään oikeutettua ja siksi suhtautuvat sen seurauksiin välinpitämättömästi. Näyttää siltä, että välinpitämättömien ryhmässä pääasiallinen tavoite ei ole saavuttaa suoranaisesti taloudellista hyötyä, joten välinpitämättömät kuuluvat voivat kuulua myös tilaisuuteen tarttujiin tai osittain ammatikseen rikoksia tekeviin. Välinpitämättömien motiivit vaikuttavat kuitenkin osittain tai välillisesti taloudellisilta, sillä toiminnan tavoite on saada ilmaiseksi jotain joka normaalisti on maksullista.

Hakkerit ovat tietoteknisesti edistyneitä henkilöitä, jotka pyrkivät testaamaan omia taitojaan erilaisien palveluiden sekä haavoittuvuuksien etsimiseen sekä järjestelmien murtamiseen. (Peltomäki & Norppa, 2015) Taylor (2005) luokittelee hakkerin ammattilaiseksi tai sisäiseksi hyökkääjäksi. Ammattilaista kuvaa vahvasti ammattitaito ja halu pyrkiä tuottamaan erilaisia rikollisia palveluita. Heillä on riittävä tietämys organisaatioiden rakenteista ja he tuntevat tavat joilla niihin voidaan murtautua. Sisäinen hyökkääjä saattaa myydä organisaatiossa tietomurtojen kautta saatua informaatiota kilpailijoille. Hakkerista on tullut yhteiskunnassa ja mediassa varsin negatiivinen sana. Hakkeri yhdistetään usein henkilöön, joka pyrkii toimimaan vihamielisesti tietojärjestelmiä vastaan ja käyttämään niitä vihamielisiin tarkoituksiin. (Kovacich, 1999) Hakkerit ovat poikkeuksellinen luokka, sillä he voivat kuulua käytännössä löyhästi kaikkiin rikollisen luokituksiin. Hakkerit voivat toimia huvittelijana, käyttäen hyväksi haavoittuvuuksia, sillä heillä on tekninen tietämys ja kyky siihen. Hakkerit voivat toisaalta toimia tarttumalla tilaisuuteen tavoitellen joitakin pieniä taloudellisia saavutuksia. Hakkerit voivat toimia osittain ammattimaisesti, jolloin he pyrkivät jonkin muun ohessa ansaitsemaan lisäansioita toteuttamalla vähäisiä kyberrikoksia. Ammattimainen verkkorikollisuus tarvitsee aina jossakin kohtaa hakkereita joilta löytyy tekninen tietämys rikoksen toteuttamiseksi, joten hakkeri voidaan tulkita ammattimaiseksi rikolliseksi. Hakkeri voi myös olla ideologiselta pohjaltaan osana jotakin ideologista järjestöä. Motiivina hakkereilla toimii taloudellisen edun tavoittelu, ideologiset taustat sekä maineen ja kunnian tavoittelu.

Ammattimainen rikollisuus verkossa on usein sidoksissa reaalimaailman hyödykkeisiin. Rikolliset voivat tehtailla erilaisia etukäteen maksettuja verkkoostoksia, joista kuluttaja ei koskaan saa ostamaansa tuotetta (Wueest, 2016). Järjestäytynyttä verkkorikollisuutta leimaa löyhästi organisoidut alihankintaverkostot, joissa haittaohjelmat ja resurssit vaihtavat omistajaa verkossa. Näissä ketjuissa tuotteita ja palvelujaan myyvät sekä menestyksekkäät hakkerit että aloittelijat, jotka käyttävät pääasiallisesti valmiiksi tuotettuja työkaluja (Jahankhani & Al-Nemrat, 2016). Tällaiset ketjut tekevät rikosten selvittämisestä todella vaikeaa, sillä syylliset ovat usein eri puolilla maailmaa ja usein jäljet päätyvät maahan, jossa viranomaisilta puuttuu tahto tai lainsäädännöllinen valtuus puuttua toimintaan (Peltomäki & Norppa, 2015). Taylor (2005), Hyppönen (2012) sekä Peltomäki ja Norppa (2015) kuvailevat kaikki rikollisia samaan tyyliin. Ammattirikolliset ovat aina taloudellisen resurssin motivoimia, toiminta on ammattimaista

sekä järjestäytynyttä ja toiminta koostuu löyhistä alihankintaverkostoista. Näyttääkin siltä, että rikollisten kuvaus on kaikissa kyberrikollisten luokitteluissa sama. Erona näyttää olevan se, että Hyppönen (2012) ei tee eroa toiminnan motiivien perusteella, vaan luokittelee kaikki rikoksia verkossa toteuttavat henkilöt rikollisiksi.

Haktivismilla tarkoitetaan väkivallatonta aktivismia, jolla pyritään vaikuttamaan poliittisesti käyttämällä lain harmaalla alueella olevia laittomia ja laillisia digitaalisia menetelmiä. (Peltomäki & Norppa, 2015) Taylor (2005) luokittelee haktivistit myös samankaltaiseen ideologiaa ohjenuorana käyttävään luokkaan aktivistit. Hyppönen (2012) luokittelee myös haktivistit omaan luokkaansa. Näin ollen voidaan sanoa, että näyttää olevan yksimielistä, että verkkorikollisten yksi luokka on ideologisesti ohjautuvat yksilöt tai ryhmät, joita voidaan kutsua haktivisteiksi. Haktivistien käyttämät menetelmät ovat tietomurrot, virtuaaliset sabotaasit, verkkosivujen turmeleminen, palvelunestohyökkäykset ja virtuaaliset istumalakot (Hampson, 2012). Haktivistijärjestöt ovat usein löyhästi organisoituja ryhmiä vailla varsinaista keskitettyä johtoa (Wueest, 2014). Haktivistijärjestöjen pysäyttäminen ja toiminnan lakkauttaminen onkin tästä syystä käytännössä mahdotonta, sillä kuka tahansa voi varsin helposti jatkaa toimintaa omilla agendoillaan. (Taylor, Jordan, & Samuel, 2004) Haktivistit kuuluvat huvittelijoihin ja ideologisiin rikollisiin toimijoihin. Haktivistit saattaisivat hyvin harvoissa tilanteissa sopia myös tilaisuuteen tarttujiin, mutta tämä on harvinaista, sillä ollakseen haktivismia on toiminnan perustuttava aina johonkin ideologiseen perustaan, joka ei synny tilaisuuden perusteella. Haktivismiin kuuluu myös olennaisesti erilainen uhittelu ja erilaisten toimijoiden uhkailu. Haktivistit ovat uhkailleet useita eri toimijoita, joista esimerkkinä voidaan pitää palvelunestohyökkäyksiä skientologien palveluihin sekä uhkausta kaataa westboro-baptist -kirkko. (Hyppönen & Tuominen, 2017)

Valtiot ovat lähteneet mukaan kyberrikollisuuteen. Valtioiden toteuttama kyberrikollisuus liittyy usein sotilaalliseen tiedusteluun ja strategisien kyberaseiden käyttämiseen. Valtiolliset toimijat saattavat toimia yrityksien kautta niin, että valtio rahoittaa yrityksen toimintaa ja yritys toimii alihankkijana. Valtiollisen toimijan tavoitteina ovat tiedustelu, teknologian ja suunnitelmien varastaminen, kybersabotaasi tai kybervandalismi (Nguyen, 2015). Valtiot hankkivat tiedustelutietoja pääasiallisesti ulkomaisista toimijoista, mutta myös oman maan kansalaisista. (Hyppönen, 2012) Valtioiden sijoittaminen rikolliseen toimintaan on hankalaa, sillä se toisaalta muistuttaa toiminnaltaan ammattimaista rikollisjärjestöä ja sen piirissä toimii ammattirikollisia, kuitenkin tämä toiminta on rikollista usein ainoastaan toiminnasta kärsivän osapuolen näkökulmasta ja valtio toimii ainoastaan omien intressejänsä mukaisesti, toteuttaen tiedustelua ja mahdollisesti taktisia kyberiskuja. Voidaankin todeta, että valtioiden motiivina kyberrikosten tehtailussa on ideologinen tai taloudellinen. Valtiot pyrkivät ajamaan omaa etuaan, johon liittyy valtion talouden kasvattaminen. Toisaalta valtio on ideologinen ihmisen luoma käsite, joten sen edun ajaminen liittyy silloin ideologisiin perusteisiin. Valtion toteuttamasta verkkorikoksesta esimerkkinä voidaan pitää stuxnet-haittaohjelmaa, jota voidaan pitää myös taktisena kyberaseena,

sillä se käytännössä toteutti samanlaisen vaikutuksen kuin kineettinen ase. Stuxnet vaurioitti Iranissa olevia uraanin rikastamiseen tarkoitettuja sentrifugeja, syöttäen niiden ohjausjärjestelmään vääriä arvoja. Stuxnetin on arvioitu olevan valtiollisen toimijan toteuttama, sillä se käytti hyväksi neljää nollapäivän haavoittuvuutta. Kukaan valtio ei ole ottanut vastuuta hyökkäyksestä, mutta tietoturva-alan ammattilaiset ovat käytännössä yksimielisiä siitä, että taustalla oli Yhdysvallat ja Israel yhdessä. (Langner, 2011)

Taulukossa 1 esitellään Taylorin (2005), Hyppösen (2012) sekä Peltomäen ja Norpan (2012) luokittelut rikollisista ja heidän motiiveistaan selkeämmässä muodossa. Taulukossa yhdistetään kyberrikolliset perinteiseen jaotteluun motiivien perusteella käyttämällä Hagan (2010) luokittelua eri rikollistyypeistä. Taulukko on itse laadittu lähteiden perusteella.

TAULUKKO 1 Kyberrikolliset, motiivit ja rikollistyyppi

Hyppönen (2012)	Peltomäki & Norppa (2015)	Taylor (2005)	Motiivi	Rikollistyyppi
Rikolliset	Tietämättömät	Mule	Taloudellinen	Osittain ammattimainen
	Välinpitämättömät	Gateway	Osittain taloudellinen	Huvittelija tai tilaisuuteen tarttuja
	Hakkerit	Insider	Taloudellinen, ideologinen	Huvittelija, tilaisuuteen tarttuja, osittain tai kokonaan ammattimainen, Ideologinen
	Ammattirikolliset	Professional	Taloudellinen	Ammattimainen
Haktivistit	Haktivistit	Activist	Ideologinen	Ideologinen ja/tai huvittelu
Valtiot	Valtiot	Nation State	Taloudellinen ja ideologinen	Ammattimainen

2.2 Kyberrikosten uhrit

Jotta voidaan ymmärtää kyberrikoksilta suojautumista ja niiden vaikutuksia, on ymmärrettävä kyberrikoksen uhreja ja uhriksi joutumista. Kyberrikollisuuden uhriksi joutuvat maailmanlaajuisesti yksityishenkilöt, yritykset sekä organisaatiot (Nykodym ym., 2005). Kyberrikoksen uhriksi joutuu päivittäin miljoona henkilöä, joista 2000-luvulla syntyneet pojat sekä kehittyvillä markkinoilla toimivat aikuiset ovat todennäköisimmät uhrit (Symantec, 2011). Symantecin (2011) teettämän tutkimuksen mukaan vastaajista 69% on joutunut kyberrikoksen uhriksi elämänsä aikana. Saman tutkimuksen mukaan viimeisen vuoden aikana kyberrikoksen uhriksi on joutunut 65% vastaajista. Kritzinger ja von Solms (2010) ovat

tutkineet kyberrikoksen uhriksi joutumisen suhdetta henkilön tietoihin sekä taitoihin. He ovat huomanneet, että organisaatioissa usein sovelletaan organisaation tietoturvakäytäntöjä. Näihin käytäntöihin kuuluvat tietoturvapolitiikka, tiedon käsittelyn prosessit, ohjesäännöt tiedon käsittelylle, hyväksi koetut tiedon käsittelyn tavat sekä tietoisuuden kasvattamista lisäävät koulutukset.

Kritzinger ja von Solms (2010) jakavat verkossa toimivat henkilöt kahteen eri käyttäjäryhmään: kotikäyttäjät (home users, HU) sekä ei-kotikäyttäjät (non-home users, NHU). On huomattava, että on mahdollista kuulua samanaikaisesti molempiin ryhmiin, jolloin organisaatiossa opitut tietoturvakäytännöt sekä tietoisuus siirtyvät myös kotikäyttäjälle. Näistä käyttäjäryhmistä kotikäyttäjät ovat merkittävästi haavoittuvampia kyberrikoksille. Tämä perustuu siihen, että kotikäyttäjiltä puuttuu riittävä tietämys uhkien ymmärtämiseen ja niiltä puolustautumiseen. Kotikäyttäjien osalta on havaittavissa, että edistyneet käyttäjät ovat myös suuremmassa vaarassa kuin he itse ovat valmiita myöntämään. Tämä johtuu siitä, että edistyneiden käyttäjien kohdalla turvallisuutta edistävät toimenpiteet usein laiminlyödään. Tällaisia turvallisuuteen liittyviä toimenpiteitä ovat tietoturvapolitiikat, hyvät salasanakäytännöt sekä käyttöjärjestelmien ja turvallisuusohjelmistojen säännöllinen päivittäminen. (Furnell, Bryant, & Phippen, 2007) Tällaisten toimenpiteiden laiminlyöminen asettaa käyttäjän sekä mahdollisesti käyttäjän organisaation riskialttiiksi taitotasosta riippumatta. Kyberrikollisuus on monella tapaa kasvoton rikos, jossa varastetaan uhreilta identiteettejä tai rahallisia resursseja. Kyberrikokset nähdään usein uhrittomana rikoksena, jossa ei ole suoranaista kärsivää kohdetta. On kuitenkin huomattavaa, että rikoksella on käytännössä aina välitön tai välillinen uhri. (Goucher, 2010) Uhrien ymmärtäminen ja jaotteleminen on yhtä tärkeää kuin rikosten tekijöiden ymmärtäminen, sillä ymmärtämällä uhriksi valikoituminen voidaan estää mahdollinen rikos sekä suojella haavoittuvia.

Joseph (2006) jakaa kyberrikollisuuden uhrit neljään luokkaan, jotka ovat herkkäuskoiset (Gullible), ahneet (Desperados), kokemattomat (Inexperienced) ja epäonniset (Unlucky people).

Herkkäuskoisilla tarkoitetaan henkilöitä, jotka saattavat aidosti uskoa verkossa tapahtuvan kanssakäymisen olevan aina totta, jolloin tällaisia henkilöitä on helppo taivutella. Herkkäuskoiset henkilöt ovat myös alttiita luovuttamaan tietojaan erilaisissa kalasteluhuijauksissa. Erityisesti lapset ja nuoret ovat riskiryhmässä, sillä he uskovat usein verkossa kaikkien olevan hyväaikeisia ja ystävällisiä. (Joseph, 2006) Näyttää siltä, että herkkäuskoiset toimivat naiivisti ja pyrkivät saavuttamaan jonkin tarpeen tyydyttämistä. Herkkäuskoiset vaikuttavat olevan alttiita aiempien rikolliskuvausten mukaan joutumaan ammattilaisten, välinpitämättömien, valtioiden sekä hakkereiden toteuttamien kyberrikosten uhriksi. Tämä johtuu siitä, että herkkäuskoisia pyritään huijaamaan verkossa toteuttamaan itse haitallinen toiminto ja motiivit vaikuttavat olevan taloudelliset. Näyttää myös siltä, että herkkäuskoiset saattavat toimia itse tietämättöminä. Herkkäuskoisten tietotaito sekä kokemus on matala, joten he kuuluvat kotikäyttäjiin. (Kritzinger & Von Solms, 2010)

Ahneilla tarkoitetaan henkilöitä, jotka ovat helpon ja nopean rahan motivoimia. Tällaiset henkilöt saattavat uskoa erilaisiin verkkohuijauksiin, joissa luvataan nopeita tuloksia sekä rahallista voittoa. Näitä huijauksia toteutetaan tietojen kalastelulla, petoksilla sekä roskapostin levityksellä. Ahneet henkilöt saattavat uskoa huijauksiin niin vahvasti, että ovat valmiita ottamaan lainaa tai myymään omaisuuttaan nopean voiton toivossa. (Joseph, 2006) Ahneet vaikuttavat toimintatapansa vuoksi joutuvan ammattilaisten, välinpitämättömien sekä hakkereiden toteuttamien kyberrikosten uhreiksi. Tämä johtuu siitä, että kyberrikosten motiivi näyttää olevan taloudellinen. Ahneet joutuvat petosten, tietojen kalastelun ja roskapostin vastaanottamisen uhreiksi. Ahneiden tietotaito ei näyttele varsinaisesti roolia rikoksen uhriksi valikoitumisessa, joten he voivat olla kotikäyttäjiä tai ei-kotikäyttäjiä. (Kritzinger & Von Solms, 2010)

Kokemattomilla tarkoitetaan henkilöitä joiden tekninen osaaminen ja ymmärrys ei ole riittävällä tasolla (Joseph, 2006). Kokemattomat joutuvat kyberrikosten uhriksi, sillä he eivät osaa edes olettaa toiminnan olevan haitallista. Kokemattomat joutuvat yleensä valtioiden, hakkereiden sekä ammattilaisten uhreiksi. Kokemattomien laitteita pyritään saastuttamaan haittaohjelmilla ja saamaan näin uhreilta tietoisesti tai huijausten kautta taloudellisia resursseja, henkilökohtaisia tietoja tai altistettua uhri petokselle. Kokemattomien tietotaito on matala ja todennäköisesti he eivät ole saaneet organisaatioiden tarjoamaa koulutusta. Kokemattomat ovat siksi kotikäyttäjiä. (Kritzinger & Von Solms, 2010)

Epäonnisilla tarkoitetaan henkilöitä, jotka ovat väärään aikaan väärässä paikassa. Epäonnisiin kuuluvat henkilöt joutuvat usein sellaisen rikoksen uhriksi, jonka välttäminen olisi käytännössä ollut mahdotonta. Epäonniseksi uhriksi saattaa valikoitua kuka tahansa tietoverkkojen käyttäjä. Epäonninen uhri joutuu tietämättömän, välinpitämättömän, hakkerin, ammattirikollisen, haktivistin tai valtiollisen toimijan uhriksi. Epäonninen uhri ei voi käytännössä välttää tilannetta. Epäonniset joutuvat haittaohjelmien, kohdennettujen hyökkäysten, palvelunestohyökkäysten sekä tietoliikenteen salakuuntelun uhreiksi. Tällaisen rikoksen uhriksi joutuvat henkilöt saattavat joutua esimerkiksi itseään tietojärjestelmässä monistavan madon uhriksi niin, että madon järjestelmään on tuonut joku kolmas osapuoli. (Joseph, 2006) Epäonnisten kohdalla tietotaito ei näyttele roolia vaan kyse on enemmänkin huonosta onnesta, siksi epäonniset voivat olla kotikäyttäjiä tai ei-kotikäyttäjiä. (Kritzinger & Von Solms, 2010)

Sukupuolisia eroja kyberrikoksen uhriksi joutumisessa näytä olevan verrattain vähän. 3% henkilöistä oli kokenut jonkin tyyppisen petoksen verkossa miehistä ja naisista. Miehistä 7% ja naisista 6% olivat joutuneet jonkin asteisen hakkeroinnin kohteeksi. Merkittävin ero kyberrikoksen uhriksi joutumisessa sukupuolten välillä on haittaohjelmatartunnoissa. Miehistä 35% oli kokenut haittaohjelmatartunnan ja naisista 27%. (McGuire & Dowling, 2013)

Taulukossa 2 esitellään kyberrikoksien uhrit sekä uhrien taitotaso käyttäen Josepsin (2006) uhriluokitusta sekä Kritzingerin ja von Solmsin (2010) tietotaitotason luokittelua. Uhrin kuvaus ja taitotaso yhdistetään todennäköisen aiemmin esiteltyihin kyberrikoksentekijöihin ja Peltomäen ja Norpan (2015) sekä McGui-

ren ja Dowlingin (2013) määrittelemiin kyberrikoksiin, joiden uhriksi uhri kuvauksensa perusteella todennäköinen joutuu. Taulukko on laadittu itse käyttäen hyödyksi edellä mainittuja lähteitä.

TAULUKKO 2 Kyberrikosten uhrit, taitotaso, todennäköinen tekijä, rikos

Uhri	**Uhrin tietotaidontaso**	**Todennäköinen rikoksentekijä**	**Rikos, jonka uhriksi todennäköisimmin uhri joutuu**
Herkkäuskoinen	Kotikäyttäjä	Ammattilainen, välinpitämätön, valtio, hakkeri	Haittaohjelmat, hakkerointi, roskapostin vastaanottaminen, motivaatiorikokset, kalastelu, petos, identiteettivarkaus,
Ahne	Ei-kotikäyttäjä ja/tai Kotikäyttäjä	Ammattilainen, välinpitämätön, hakkeri	Petos, kalastelu, roskapostin vastaanottaminen
Kokematon	Kotikäyttäjä	Hakkeri, valtio, ammattilainen	Haittaohjelmat, kalastelu, petos
Epäonninen	Ei-kotikäyttäjä ja/tai Kotikäyttäjä	tietämättömät, välinpitämättömät, hakkerit, ammattirikolliset, haktivistit, valtiot	Petos, Haittaohjelmat, kohdennetut hyökkäykset, palvelunesto, tietoliikenteen salakuuntelu

3 KYBERRIKOLLISTEN TOIMINTATAVAT

Kyberrikollisuudella tarkoitetaan yksinkertaisimmillaan rikoksia, jotka toteutetaan tietoverkkojen avulla. (Nykodym ym., 2005). Useimmissa kyberrikollisuuden määritelmissä halutaan kuitenkin tehdä selkeä ero teknisten rikosten ja teknologia-avusteisien rikosten välille. Viestintävirasto (2016c) jakaa tietoverkoissa tapahtuvan rikoksen kahteen eri luokkaan, tietokoneavusteisiin rikoksiin ja tietotekniikkarikoksiin. Tietokoneavusteiset rikokset vastaavat määrittelyltään kyberavusteisia rikoksia, eli rikoksia, joissa rikos voitaisiin toteuttaa myös ilman tietokoneita ja tietoverkkoja. Tietotekniikkarikoksilla tarkoitetaan rikoksia, jotka vastaavat kyberriippuvaisen rikoksen määritelmää. Kyberriippuvaiset rikokset ovat rikoksia, joiden toteuttaminen ilman tietoverkkoja ja tietokoneita on mahdotonta. Gordon ja Ford (2006) jakavat rikokset kohteen perusteella kahteen luokkaan. He jakavat kyberrikollisuuden teknologiarikoksiin (Technology crime), jotka kohdistuvat teknologisiin resursseihin sekä ihmisiin kohdistuviin rikoksiin (people crime), jossa kyberrikosten kohteena on ihminen. McGuire ja Dowling (2013) kuvailevat teknologiaan kohdistuvia ja teknologiaa hyödyntäviä rikoksia nimikkeillä kyberriippuvaiset rikokset (Cyber-Dependent Crimes) tai puhtaat kyberrikokset (Pure Cyber Crime). Kyberriippuvaiset rikokset pyritään ensisijaisesti ohjaamaan tietojenkäsittely- tai verkkoresursseja vastaan ja ne toteutetaan informaatioteknologian avulla. Näyttää siltä, että kaikissa kyberrikollisuuden määritelmissä tehdään erottelu teknologisten ja ihmisiin suoraan kohdistuvien rikosten välille. Teknologiarikoksia leimaa tarve käyttää tietokoneita tai tietoverkkoja rikoksen tekovälineenä ja niiden toteuttaminen ei ole mahdollista ilman niitä. Kyberavusteiset rikokset näyttävät olevan perinteisiä rikoksia jotka toteutetaan uudessa ympäristössä. Tällaisia rikoksia ovat esimerkiksi petokset verkon sähköisillä markkinapaikoilla. Poliisi on arvioinut yli puolien suomessa tapahtuvien petosten tapahtuvan verkossa. (Viestintävirasto, 2016e)

Taulukossa 3 esitellään kyberrikosten määritelmät ja niiden yhteneväisyydet verraten niitä kyberriippuvaisiin ja kyberavusteisiin rikoksiin. Taulukko on laadittu itse käyttäen hyödyksi taulukossa mainittuja lähteitä.

TAULUKKO 3 Kyberrikosten luokittelut

	Kyberriippuvaiset rikokset	**Kyberavusteiset rikokset**
Viestintävirasto (2016)	Tietotekniikka rikokset	Tietokoneavusteiset rikokset
Gordon ja Ford (2006)	Teknologia rikos	Ihmisiin kohdistuva rikos
McGuire ja Dowling (2013)	Puhtaat kyberrikokset	-

3.1 Kyberavusteiset rikokset

Viestintäviraston (2016c) määritelmän mukaan jos rikos on toteutettavissa reaalimaailmassa myös ilman tietoverkkojen sekä tietokoneiden avustusta on kyseessä kyberavusteinen rikos. Kyberavusteiset rikokset ovat käytännössä aiemmin tunnettuja rikostyyppejä, joita toteutetaan uudessa ympäristössä, sillä se on kustannustehokasta. Kyberavusteisia rikoksia ovat mm. tietoverkossa tapahtuva petos, tietojenkalastelu sekä identiteettivarkaus.

Kyberavusteinen petos tapahtuu usein reaalimaailman hyödykkeellä tai omaisuuserällä ja sen anastaminen tai huijaaminen on mahdollista myös reaalimaailmassa. (Peltomäki & Norppa, 2015) Kyberavusteisten petosten tekijät ovat usein ns. pikkurikollisia ja niihin liittyy vähäisessä määrin ammattimaista rikollisuutta. Tällaisia rikoksia saattavat olla tietämättömien ja välinpitämättömien toteuttamat vähäiset petokset sähköisillä markkinapaikoilla. Ammattimaisemmassa rikollisuudessa toimintaan liittyy usein maksukorttipetokset. Rikolliset voivat tehtailla erilaisia etukäteen maksettuja verkko-ostoksia, joista kuluttaja ei koskaan saa ostamaansa tuotetta. Tällaisten kyberavusteisten rikosten arvoksi on arvioitu vuonna 2011 noin miljardi dollaria (Anderson ym., 2012). Kyberavusteisten petosten uhreiksi joutuvat herkkäuskoiset, ahneet sekä kokemattomat.

Tietojenkalastelulla tarkoitetaan arvokkaan henkilökohtaisen tai organisaatioon liittyvän tiedon keräämistä. Tällaisia tietoja ovat syntymäajat, koko nimet, vanhempien omat sukunimet (tyttönimet), tilitiedot, salasanat, sähköpostiosoitteet sekä henkilötunnukset. Tietojenkalastelu koostuu kahdesta eri prosessista. Ensimmäisessä vaiheessa tietoja pyritään saamaan rikollisten haltuun (Jahankhani & Al-Nemrat, 2016). Rikolliset käyttävät toimintatapana toisinaan hyvinkin tökerösti ja huonosti kirjoitettuja viestejä, joissa luvataan jotain mikä ei ole totta. Viestintämenetelminä käytetään roskapostia, huijausta varten rakennettuja verkkosivuja sekä puhelimella soittamista. (Abbasi ym., 2010) Toisessa vaiheessa tietoa pyritään hyödyntämään ja saavuttamaan sillä etuja (Jahankhani & Al-Nemrat, 2016). Uhrien käyttäjätunnuksilla voidaan kirjautua sähköpostipalveluun ja valjastaa uhrin sähköposti lähettämään roskapostia, uhrin nimissä saatetaan tilata hänen luottokortillaan hyödykkeitä tai manipuloida uhri soittamaan maksulliseen numeroon. (Viestintävirasto, 2016b) Tietojen kalastelua harjoittavat rikollisista ammattilaiset, sillä tietojenkalastelun tarkoituksena on hyödyntää niitä myöhemmin taloudellisesti. Tietojenkalastelun uhriksi joutuvat usein heikon tietotaidon omaavat henkilöt. Ammattirikollisten toteuttamien tietojenkalastelujen uhreiksi joutuvat tästä syystä herkkäuskoiset ja kokemattomat.

Identiteettivarkauksia tapahtuu myös reaalimaailmassa, kun identiteetintunnistamisvälineitä tai -dokumentteja kadotetaan tai ne varastetaan. Identiteettivarkaus on kriminalisoitu Suomessa vasta vuonna 2015. Identiteettivarkaudesta on säädetty Suomen rikoslaissa tieto- ja viestintärikoksissa 38 luvussa § 9 identiteettivarkaus rikokseksi, jossa tekijä erehdyttää kolmatta osapuolta oikeudettomasti käyttämällä toisen henkilön henkilötietoja, tunnistamistietoja tai

muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee. Identiteettivarkaudesta suomessa voidaan tuomita sakkoihin. Vuonna 2015 identiteettivarkauksia ilmoitettiin poliisille 554 kappaletta ja vuonna 2016 2222 kappaletta. Nopeasti pääteltynä hälyttäväksi voitaisiin huomata räjähdysmäinen kasvu, mutta syvällisemmän tarkastelun perusteella identiteettivarkauksien suuri ero vuosien välissä johtuu siitä, että identiteettivarkaudet on kriminalisoitu vasta loppuvuodesta 2015, jolloin vuoden keskiarvo muille kuukausille on samaa luokkaa kuin vuonna 2016. (Liite 1) Identiteettivarkaudet liittyvät yleensä varsin pieniin summiin ja niitä tehtaillaan saavuttaen vain pieni taloudellisia hyötyjä. Varastetun identiteetin turvin saatetaan ostaa hyödykkeitä verkosta, nostaa korkeakorkoisia kulutusluottoja, avata puhelinliittymiä sekä ostaa liittymään sidottuja puhelimia. Identiteettivarkauden uhriksi joutuvat henkilöt, jotka luovuttavat kalasteluissa henkilötietojaan tai joutuvat tietomurtojen kohteiksi. Identiteettivarkauden kautta saavutettu taloudellinen hyöty on kuitenkin usein varsin vähäistä, sillä uhrin nimissä ehditään usein tehdä vain muutamia rikoksia. Rikollisten tavoite on saavuttaa pieniä taloudellisia hyötyjä, jolloin rikolliset ovat välinpitämättömiä tai ammattirikollisia riippuen toiminnan laajuudesta.

Taulukossa 4 esitellään kyberavusteiset rikokset. Ensimmäisessä sarakkeessa ovat Peltomäen ja Norpan (2015) esittelemät rikokset, toisessa sarakkeessa aiemmin esitellyt tekijät, jotka todennäköisimmin syyllistyvät rikokseen, kolmannessa sarakkeessa aiemmin esitelty rikoksen motiivi ja neljännessä sarakkeessa todennäköisin uhri rikokselle käyttäen Josepsin (2016) kuvausta uhreista. Taulukko on laadittu itse selkeyttämään kyberavusteisien rikosten hahmottamista.

TAULUKKO 4 Kyberavusteiset rikokset, tekijät, motiivit ja uhrit:

Rikos	**Tekijä**	**Motiivi**	**Rikoksen todennäköinen uhrit**
Kyberavusteinen petos	Tietämätön, Välinpitämätön tai ammattirikollinen	Taloudellinen	Herkkäuskoinen, ahne ja kokematon
Kyberavusteinen tietojenkalastelu	Ammattirikollinen	Taloudellinen	Herkkäuskoinen ja kokematon
Kyberavusteinen identiteettivarkaus	Välinpitämättömiä ja ammattirikollisia	Taloudellinen	Herkkäuskoinen, kokematon ja epäonninen

3.2 Kyberriippuvaiset rikokset

Kyberriippuvaisilla rikoksilla tarkoitetaan laitonta toimintaa, joka vaatii tietoverkon tai tietokoneen rikoksentekovälineenä. Kyberriippuvaiset rikokset jaotellaan kuuteen eri alakategoriaan: haittaohjelmien kehitys ja hyödyntäminen, hakkerointi, palvelunestohyökkäykset, roskapostin levittäminen, botnettien luominen ja hallinnointi sekä motivaatiorikokset. Kyberriippuvaisten rikosten motiivina toimivat taloudellisen edun tavoittelu, poliittiset ja ideologiset motiivit sekä vandalismi (Viestintävirasto, 2016e).

Haittaohjelmalla tarkoitetaan tietokoneohjelmaa jolla on haitallisia toimintatapoja. Aiemmin haittaohjelmat jaettiin kolmeen luokkaan: virukset, madot ja troijalaiset. (Christodorescu, Jha, Seshia, Song & Bryant, 2005) Haittaohjelmat jaotellaan nykyisin kuitenkin neljään kategoriaan: virukset, madot, troijalaiset sekä spywaret (Choo, 2011a). Spywaren lisääminen luokitteluun johtuu big datan lisääntymisestä ja käyttäjätiedon merkittävyyden kasvusta. Virukset ovat mediassa usein esiintyvin haittaohjelma luokka joille tunnuksenomaista on niiden leviäminen tietokoneiden välityksellä sekä niiden kyky monistaa itseään. Virukset vaativat aina isäntätiedoston, levyn tai dokumenttitiedoston, jonka välityksellä ne leviävät. Viruksille tunnusomaista on se, että ne eivät voi levitä ilman, että ihminen osallistuu prosessiin tahattomasti tai tahallisesti. (Moir, 2013). Madot ovat itseään monistavia ohjelmia, jotka leviävät järjestelmien välillä vaatimatta ihmisten osallistumista toimintaa. Madot pyrkivät leviämään järjestelmässä käyttämällä hyödyksi järjestelmän omia tiedonsiirtomenetelmiä. Tästä syystä madot saattavat pysyä huomaamattomina järjestelmissä pitkiäkin aikoja ja aiheuttaa laajaa vahinkoa koko järjestelmässä. Yksinkertainen esimerkki madon leviämisestä on sähköpostin välityksellä leviävä mato, joka lähettää itsensä koko osoitekirjalle tarttuessaan. (Beal, 2004) Troijalaisilla tarkoitetaan ohjelmia, jotka esiintyvät ensin täysin hyödyllisinä ja käyttökelpoisina ohjelmina, jotka muuttuvat ohjelman suorituksen aikana vihamieliseksi. Troijalaiset avaavat takaoven uhrin tietokoneeseen, varastavat tietoja sekä suorittavat legitiimin prosessin aikana piilotettuja vihamielisiä toimintoja. (McGuire & Dowling, 2013) Spyware on haittaohjelma, jonka tarkoituksena on kerätä käyttäjästä arkaluontoista tai henkilökohtaista tietoa saastuneen tietojärjestelmän kautta. Informaatiota voidaan kerätä useilla eri tavoilla. Käyttäjää voidaan vakoilla käynnistämällä tietokoneen kamera, mikrofoni tai tallentamalla näppäinten painalluksia käyttämällä keylogger-tekniikoita. Tällaiset näppäinten tallennusohjelmistot tallentavat käyttäjän näppäimistön painallukset ja niiden tavoitteena on saada haltuun käyttäjätunnuksia, salasanoja sekä luottokortti- ja pankkitietoja. (McGuire & Dowling, 2013) Spyware-vakoiluohjelmia pidetään yhtenä vaarallisimmista haittaohjelmien muodoista, sillä niiden pääasiallinen tarkoitus on käyttäjän yksityisyyden rikkominen (Jewkes & Yar, 2013). Haittaohjelmien kehittäminen vaatii edistynyttä tietoteknistä osaamista. Haittaohjelmien kehittäminen vaatii ohjelmointitaitojen lisäksi myös edistynyttä tietoutta tietoverkkojen ja -järjestelmien toiminnasta.

Haittaohjelmien levittäminen sen sijaan ei välttämättä vaadi kovinkaan edistyksellistä tietoteknistä osaamista, sillä haittaohjelman levittämiseen riittää houkuttelevaan muotoon kirjoitettu sähköposti. Haittaohjelmien kehittämiseen syyllistyvät tietoteknisesti edistykselliset hakkerit ja niiden levittämiseen hakkerit sekä ammattirikolliset. Valtioiden tunnetaan myös kehittäneen omia haittaohjelmia tiedusteluun sekä taktisiksi kyberaseiksi. Haittaohjelmilla tavoitellaan ideologista tai taloudellista päämäärää. (Langner, 2011) Haittaohjelmien uhriksi joutumiseen ei ole olemassa suoraa kaavaa, sillä haittaohjelmat pyrkivät leviämään mahdollisimman tehokkaasti. Haittaohjelmien uhriksi joutuvat tästä syystä herkkäuskoiset, ahneet, kokemattomat ja epäonniset.

Hakkeroinnilla tarkoitetaan hakkerin tunkeutumista tietokoneeseen, tietojärjestelmään tai -verkkoon sen ulkopuolelta ilman auktorisoitua lupaa. Järjestelmään murtautuminen mahdollistaa sen katselun ja tutkimisen sisältäpäin. Tämän lisäksi hakkerointi mahdollistaa myös vahingollisemmat toiminnot kuten tietojen muokkaamisen, kopioinnin tai hävittämisen, järjestelmän ja/tai prosessin vakoilun tai laittoman sisällön jakamisen järjestelmän avulla. (Limnéll ym., 2014, s. 236). Hakkerointiin liittyvä motiivi voi liittyä taloudellisen edun tavoitteluun rikollisin keinoin, jolloin kyseessä on niin sanottu mustahattuhakkerointi (black hat hacker) tai valkohattuhakkerointiin (white hat hacker), jolloin tavoitteena on järjestelmän turvallisuuden parantaminen. Black hat -hakkereita työllistävät usein rikollisjärjestöt ja white hat -hakkereita yksityiset turvallisuus-alan yritykset. (Brown, 2015) Hakkeroinnilla tavoitellaan yleisimmin taloudellista etuutta, mutta hakkerointia saatetaan tehdä myös ideologisesta motiivista, huvin vuoksi tai näyttämisen halusta. Hakkerointi vaatii teknisesti edistyksellisen henkilön, jota kutsustaan hakkeriksi. Hakkeri saattaa kuitenkin työskennellä ammattirikollisille tai valtiolliselle toimijalle. Hakkeroinnin uhriksi voi periaatteessa joutua kuka tahansa yksityishenkilö tai organisaatio, kuitenkin näyttää siltä hakkerit pyrkivät valitsemaan uhrikseen mahdollisimman helpon kohteen (Hyppönen & Tuominen, 2017). Tästä syystä uhreiksi joutuvat useimmiten kokemattomat ja huono-onniset.

Palvelunestohyökkäyksellä tarkoitetaan hyökkäystä jossa uhrin palvelinta, tietoverkkoa tai tietojärjestelmää kohtaan kohdistetaan hyökkäys joka estää sitä suoriutumasta normaalista tehtävästään (Chang, 2002). Palvelunestohyökkäyksiä voidaan toteuttaa hajautetusti (Distributed Denial of Service, DDoS) tai keskitetysti (Denial of Service, DoS) (Durcekova, Schwartz, & Shahmehri, 2012). Palvelunestohyökkäyksellä ei kuitenkaan tarkoiteta palveluun murtautumista vaan palvelunestohyökkäyksellä voidaan ainoastaan estää muita käyttäjiä saavuttamasta palvelua. Palvelunestohyökkäysten osalta on kuitenkin tiedostettava, että niitä saatetaan käyttää hämäyksenä, jonka avulla saadaan kiinnitettyä ylläpidon huomio muualle kuin varsinaiseen hyökkäykseen. Palvelunestohyökkäyksien motiivina toimii usein kiusanteko, julkisuushakuisuus, haktivismi tai muut poliittiset motiivit. Motiivina saattaa olla myös esimerkiksi kilpailijan verkkokaupan häiritseminen vuoden vilkkaimpana myyntipäivänä. (Viestintävirasto, 2016d) Hajautetusta palvelunestohyökkäyksestä esimerkkinä voidaan käyttää Virossa keväällä 2007 nähtyjä hyökkäyksiä pronssipatsaskiistan aikana. Viron

valtion verkkosivuilla vierailee normaaleissa oloissa n. 1000 kävijää päivittäin, kun hajautetun palvelunestohyökkäyksen aikana siellä saavutettiin keskimäärin 2000 kävijän sekuntivauhti (Wilson, 2008). Palvelunestohyökkäyksen laajuuden vuoksi on esitetty epäilyjä, että se olisi poliittisesti/ideologisesti motivoitunut ja siksi valtion toteuttama. Tästä ei kuitenkaan ole olemassa varmaa näyttöä, mikä on tyypillistä kyberrikoksille. Kaiken kaikkiaan hajautetussa palvelunestohyökkäyksessä Viroon kohdistui liikennettä 197 eri valtion verkkoavaruudesta (Candolin, 2012). Palvelunestohyökkäyksiä voi tällä hetkellä ostaa tuntilaskutuksella tietoverkkorikollisilta (Hyppönen & Tuominen, 2017). Palvelunestohyökkäyksissä motiivi näyttää olevan ideologinen tai taloudellinen. Näistä esimerkkinä toimivat lukuisat Anonymous-ryhmän toteuttamat palvelunestohyökkäykset (Webster, 2012). Palvelunestohyökkäyksien helpon saatavuuden vuoksi niitä toteuttavat hakkerit, välinpitämättömät, ammattirikolliset, haktivistit sekä valtiot. Palvelunestohyökkäysten kohteeksi tai vaikutuksenalaiseksi joutuvat kaikki jotka ovat osana palvelun käyttäjiä tai tarjoajia. Näin ollen palvelunestohyökkäysten uhreiksi joutuvat kaikki uhriryhmät.

Roskapostin levittämisellä tarkoitetaan ei-toivottujen sähköpostien lähettämistä suurelle vastaanottajajoukolle. Roskapostit sisältävät mainoksia tai kalasteluviestejä. (Peltomäki & Norppa, 2015, s. 171) On arvioitu, että yli 90% kaikesta verkossa tapahtuvasta sähköpostiviestinnästä on roskapostia (Lindford, 2016). Roskapostien tavoitteena on saavuttaa taloudellista etua ohjaamalla käyttäjä ostamaan tuote tai luovuttamaan ammattirikollisille tietoja joita voidaan käyttää hyödyksi. Roskapostin tunnistaminen ei usein ole kovinkaan hankalaa, joten rikoksen uhriksi joutuvat herkkäuskoiset sekä kokemattomat.

Bottiverkolla tarkoitetaan joukkoa haittaohjelmilla saastutettuja tietokoneita, jotka on liitetty yhteen tietoverkon avulla. Bottiverkkojen ylläpitämisellä ja luomisella tavoitellaan pääasiallisesti hajautettujen palvelunestohyökkäysten tai roskapostin levittämiseen perustetun infrastruktuurin luomista. (Peltomäki & Norppa, 2015) Bottiverkkoja pyrkivät rakentamaan ammattirikolliset sekä hakkerit, sillä niitä voidaan myydä taloudellisin motiivein tuntilaskutuksena. Bottiverkkojen uhreiksi joutuvat välillisesti kaikki palvelunestohyökkäyksistä kärsivät henkilöt. Suoranaisesti bottiverkkojen uhreiksi joutuvat henkilöt, joiden laitteet on valjastettu haittaohjelmin mukaan bottiverkkoon. Haittaohjelman saaminen voi olla monesta tekijästä kiinni, joten bottiverkkojen uhriksi voivat joutua kaikki uhriryhmät. Suurimpia bottiverkkoja ovat olleet Mirai, joka saastutti internet of things -laitteita kuten turvakameroita. Työasemia saastuttanut laajalle levinnyt esimerkki on ZeroAccess, joka on saastuttanut ainakin n. 2 miljoonaa työasemaa. On myös arvioitu, että sen kuluttamalla energialla voitaisiin lämmittää 111 000 kotia joka päivä (Thomas, 2016).

Motivaatiorikoksilla tarkoitetaan sellaisia rikoksia, jotka perustuvat henkilökohtaiseen tietotarpeeseen tai rahalliseen hyötyyn (McGuire & Dowling, 2013). Tällainen rikos voi olla esimerkiksi mustasukkaisen aviopuolison asentama haittaohjelma puolison matkapuhelimeen, jonka perusteella hänen sijaintiaan, puhelimen sisältöä tai valokuvia voidaan vakoilla. Muita syitä motivaatiorikoksille

saattavat olla muun muassa kosto, mielenkiinto, kunnioituksen haku, vallan tavoittelu organisaatiossa tai hyvin yksinkertaisesti tylsyys. (Kirwan & Power, 2011) Motivaatiorikoksia ohjaa usein vahva ideologinen peruste ja niiden tekijät tietävät toimivansa väärin, mutta uskovat tarkoituksen pyhittävän keinot. Rikoksen uhriksi joutuu käytännössä aina huono-onninen henkilö.

Taulukossa 5 esitellään kyberriippuvaiset rikokset. Ensimmäisessä sarakkeessa ovat Peltomäen ja Norpan (2015) esittelemät rikokset, toisessa sarakkeessa aiemmin esitellyt tekijät jotka todennäköisimmin syyllistyvät kyberriippuvaiseen rikokseen, kolmannessa sarakkeessa aiemmin esitelty rikoksen motiivi ja neljännessä sarakkeessa todennäköisin uhri rikokselle käyttäen Josepsin (2016) kuvausta uhreista. Taulukko on laadittu itse selkeyttämään kyberriippuvaisten rikosten hahmottamista.

TAULUKKO 5 Kyberriippuvaiset rikokset, tekijät, motiivit ja uhrit:

Rikos	**Tekijä**	**Motiivi**	**Rikoksen todennäköiset uhrit**
Haittaohjelmat	Hakkerit, ammattirikolliset ja valtiot	Taloudellinen	Herkkäuskoiset, ahneet, kokemattomat ja huono-onniset
Hakkerointi	Hakkerit, ammattirikolliset ja valtiot	Ideologinen ja/tai taloudellinen	kokemattomat ja huono-onniset
Palvelunestohyökkäykset	Hakkerit, välinpitämättömät ammattirikolliset, haktivistit ja valtiot	Ideologinen ja/tai taloudellinen	Herkkäuskoiset, ahneet, kokemattomat ja huono-onniset
Roskapostin levittäminen	Ammattirikolliset	Taloudellinen	Herkkäuskoiset, ahneet ja kokemattomat
Bottiverkot	Hakkerit ja ammattirikolliset	Taloudellinen	Herkkäuskoiset, ahneet, kokemattomat ja huono-onniset
Motivaatiorikokset	Välinpitämättömät	Ideologinen	Huono-onniset

3.3 Kyberrikollisuus Suomessa

Poliisiammattikorkeakoulun tilastopalvelulta tilatun aineiston mukaan kyberrikollisuus on kasvanut Suomessa vuosien 2000 – 2015 välillä noin seitsemän prosentin vuosivauhdilla (Liite 1: poliisiammattikorkeakoulu, 2016). Kyberavusteisista rikoksista eniten näinä vuosina on rikosilmoituksia tehty viestintäsalaisuuden loukkauksesta, jolla tarkoitetaan oikeudettomasti toiselle kuuluvan informaation avaamista tai muun vastaavan suljetun viestin salauksen purkamista (Rikoslaki 38 10.4.2015/368 3 §). Rikos voi tapahtua reaalimaailmassa paperisella kirjeellä tai sähköisessä muodossa olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron sisällön laittomalla avaamisella (Oikeusministeriö, 2000). Tällaisia rikosilmoituksia on kirjattu poliisiammattikorkeakoulun tilastopalvelun mukaan 3466 kappaletta vuosien 2000 ja 2015 välillä. Kyberriippuvaisista rikoksista eniten rikosilmoituksia on tehty tietomurroista vuosien 2000 ja 2015 välillä. Tietomurroista rikosilmoituksia on ilmoitettu 3488 kappaletta. Tietomurrolla (Rikoslaki 10.4.2015/368 8 §) tarkoitetaan rikosta, jossa henkilö käyttää hänelle kuulumatonta käyttäjätunnusta tai muuten tunkeutuu tietojärjestelmään, johon hänellä ei ole riittäviä oikeuksia. Rikoksessa voidaan hyväksi käyttää myös teknisiä keinoja turvajärjestelmien ohittamiseksi tietokonejärjestelmien haavoittuvuuksia hyväksikäyttäen (Oikeusministeriö, 2015).

4 KYBERRIKOKSILTA SUOJAUTUMINEN

Yhdysvalloissa FBI:n johtaja James Comey (2014) totesi maailmassa olevan kahdenlaisia yrityksiä, niitä jotka on hakkeroitu ja niitä, jotka eivät vielä tiedä siitä. Kyberrikosten määrä tulee tulevien vuosien aikana kasvamaan merkittävästi (Choo, 2011b) yksilöiden, yritysten ja organisaatioiden on otettava kyberuhat ja kyberrikollisuus vakavasti. Kyberuhilta voidaan suojautua ja kyberpuolustusta voidaan kehittää seuraamalla alalle kehitettyjä standardeja sekä hyviä käytäntöjä. Kyberrikoksen uhriksi joutumisesta on myös opittava ja organisaatioiden on panostettava toiminnan jatkumiseen, vaikka kyberrikos onkin tapahtunut. (Viestintävirasto, 2010)

4.1 Yksityishenkilö

Kuluttajat voivat suojautua kyberrikollisuutta vastaan seuraamalla yleisesti hyväksi koettuja tietoturvaohjeistuksia joita antaa suomessa mm. viestintävirasto. Peruskäytäntöihin kuuluvat käyttöjärjestelmän, tietoturvaohjelmien sekä internetselainten päivitykset. Näistä on huolehdittava säännöllisesti. Käyttäjän on tarkistettava tapahtuuko päivittäminen automaattisesti vai tarvitaanko siihen käyttäjältä toimenpiteitä. Käyttäjien heikko tietoturvatietoisuus on usein syynä rikoksen uhriksi joutumiseen. Tietoturvatietoisuuden kasvattamisella voidaan ehkäistä valtaosa rikoksista. (Kritzinger & Von Solms, 2010)

Sähköpostin liitetiedostoja ei tule koskaan avata, mikäli on epävarmuutta mitä ne sisältävät. (Peltomäki & Norppa, 2015) Lähettäjä on varsin helposti manipuloitavissa, joten siihen ei tule luottaa. (The Federal Bureau of Investigation, 2016) Peltomäen ja Norpan ohjetta tukee myös Nelmsin (1999) tekemä havainto, jonka mukaan liitetiedostoissa leviävät haittaohjelmat usein aiheuttavat välitöntä haittaa tietojärjestelmälle, sillä ne saattavat sisältää suoritettavaa ohjelmakoodia myös taulukkolaskennan tai tekstitiedoston makroissa. Yleensä tällaiset haittaohjelmat ovat viruksia, matoja tai troijalaisia. (Nelms, 1999) Kiristyshaittaohjelmia on mm. levitetty käyttämällä hyväksi liitetiedostojen makroja (Viestintävirasto, 2016c). Sähköpostin välityksellä haittaohjelmia pyrkivät levittämään ammattirikolliset, hakkerit sekä valtiot. Sähköpostin välityksellä leviävien haittaohjelmien motiivina on taloudellinen motiivi ja niiden uhriksi joutuvat herkkäuskoiset, ahneet, kokemattomat sekä huono-onniset. (Joseph, 2006)

Roskapostiviesteihin ei tule vastata. Niihin vastaaminen osoittaa sähköpostilaatikon olevan aktiivinen ja siihen ryhdytään kohdistamaan jatkossa lisää roskapostia. (Peltomäki & Norppa, 2015) Viestintävirasto ohjeistaa myös vastaamatta jättämisen lisäksi tarkkaan harkitsemaan mihin luovuttaa sähköpostitietojaan. Roskapostin vastaanottamista voidaan vähentää merkittävästi mikäli osoite ei päädy roskapostittajien osoitteistoon. (viestintävirasto, 2003) Mikäli käyttäjä

alkaa kuitenkin saamaan roskapostia, voidaan roskapostin saamista yrittää vähentää asettamalla sähköpostiin suodattimia estämään erilaisia sanoja jotka esiintyvät roskaposteissa usein. Usein kuitenkin roskapostista lähetetään useita eri versioita, joissa saattaa esiintyä muunnoksia sanoista. Tällaisesta esimerkki voi olla esimerkiksi ”viagran” sijasta kirjoitettu ”v!agra.” (Vorakulpipat, Visoottiviseth, & Siwamogsatham, 2012) Roskapostin tunnistamisella ja vastaamatta jättämisellä voidaan ehkäistä henkilön altistumista muille rikoksille. Roskapostin levittämiseen syyllistyvät ammattirikolliset, joiden motiivina on taloudellinen hyöty. (Peltomäki & Norppa, 2015) Roskapostia saattaa vastaanottaa kuka tahansa, mutta roskapostin ohjaamaan toimintaan ryhtymiseen alttiimpia ovat herkkäuskoiset, ahneet sekä kokemattomat. (Joseph, 2006)

Tietokoneella on oltava asennettuna tietoturvaohjelmistot sekä asetukset. Tällaisia ovat palomuuri sekä virustorjunta. Tietoturvaohjelmistojen ja käyttöjärjestelmän päivitykset on pidettävä ajan tasalla. (Peltomäki & Norppa, 2015) Tietoturvaohjelmistojen ja palomuurien päivittäminen perustuu tunnettujen haavoittuvuuksien julkaisuun. Käyttöjärjestelmissä havaitut haavoittuvuudet julkaistaan usein, kun jokin ennalta ilmoitettu aika (usein 12 viikkoa) on kulunut haavoittuvuuden raportoimisesta. Päivitykset ja ohjelmistokoodien virheiden korjaukset korjaavat tällaisia haavoittuvuuksia ja siitä syystä korjausten saaminen on mahdollista ainoastaan pitämällä järjestelmät päivitettyinä. (Pounder, 2002) Haittaohjelmat tarttuvat koneisiin useimmiten sähköpostin liitetiedostona tai epämääräiseltä verkkosivustolta (Viestintävirasto, 2016c). Käyttäjän saadessa haittaohjelmainfektio, on kone irrotettava verkosta ja siihen on ajettava päivitetyllä tietoturvaohjelmistolla virustarkistus. Vaikka haittaohjelma saataisiinkin poistettua, on tietokone hyvä alustaa uudelleen ja ottaa käyttöön vasta sen jälkeen. (Peltomäki & Norppa, 2015) Asianmukaisilla tietoturvaohjelmistoilla sekä tietoturvatietoisuudella voidaan suojautua tehokkaasti haittaohjelmilta, hakkeroinnilta, bottiverkoilta sekä motivaatiorikoksilta, sillä nämä kaikki ovat toteutettavissa haittaohjelmin. (McGuire & Dowling, 2013) Tietoturvaohjelmistoilla voidaan suojautua ammattirikollisilta, hakkereilta ja välinpitämättömiltä. Haittaohjelmin toteutettavien rikollisten uhreiksi joutuvat herkkäuskoiset, ahneet, kokemattomat sekä huono-onniset. (Joseph, 2006)

Mobiililaitteet ovat nykyisin osa ihmisen identiteettiä ja mobiililaitteilla voidaan hoitaa mm. henkilöllisyyden todistaminen pankkipalveluiden avulla tai mobiilivarmenteella. Mobiililaitteet on suojattava kaikissa tilanteissa salasanalla, pääsykoodilla ja/tai sormenjäljellä. Mobiililaitteet eivät ole ikuisia. Mobiililaite saatetaan varastaa tai käyttäjä saattaa kadottaa tai hajottaa laitteen. Laitteen osalta on huolehdittava varmuuskopioinnista, jotta käyttäjälle tärkeitä tietoja ei pääse katoamaan. Mobiililaitteita myydään ja ostetaan myös käytettyinä. Mobiililaitetta myyvän käyttäjän on pidettävä huolta omasta tietoturvastaan tällaisissa tilanteissa. Mobiililaite on kytkettävä pois pilvipalveluista, tyhjennettävä laitteen sisäinen muisti ja mahdollisesti lisämuistina toimiva muistikortti. Puhelin on myös palautettava tehdasasetuksille. Käyttäjä pystyy näin suojautumaan esimerkiksi identiteettivarkaudelta. (Olin, 2014) Mobiililaitteiden osalta on tutustuttava

tietoturvaohjelmistoihin mikäli sellaiseen on tarvetta. Mobiililaitteissa on tarkistettava tietoturva-asetukset. Android -järjestelmiä ei tule koskaan käyttää ilman asianmukaista tietoturvaohjelmistoa. (Peltomäki & Norppa, 2015) Haittaohjelmainfektiota voi epäillä mobiililaitteessa, mikäli puhelimen käyttö hidastuu merkittävästi ja sen uudelleenkäynnistys ei poista ongelmaa, puhelimen käyttöjärjestelmässä esiintyy poikkeuksellisen usein kaatumisia tai mobiililaite kuluttaa akkua merkittävästi nopeammin kuin aikaisemmin. Mobiililaitteen saastuessa se on puhdistettava antivirusohjelmalla sekä palautettava tehdasasetuksille. (Olin, 2014) Mobiililaitteiden turvallisuudesta huolehtimalla voidaan suojautua välinpitämättömien ja ammattirikollisten toteuttamia kyberavusteisia identiteettivarkauksia sekä haittaohjelmia vastaan. Suojatulla mobiililaiteella voidaan ehkäistä myös motivaatiorikoksia. (McGuire & Dowling, 2013)

Käyttäjän tunnistamiseen verkon palveluissa käytetään yleisesti käyttäjätunnus ja salasana -paria. Tällaista tunnistamista kutsutaan heikoksi tunnistamiseksi, sillä se vaatii ainoastaan yhden tunnistamisen menetelmän. Vahvalla tunnistamisella tarkoitetaan tilannetta, jossa kaksi kolmesta vahvan tunnistamisen periaatteesta ovat voimassa. Vahvan tunnistamisen periaatteessa tunnistaminen perustuu käyttäjän omaan tietoon (esim. salasana), käyttäjän hallussa olevaan tietoon (esim. sirukortti) ja käyttäjän biometriseen ominaisuuteen (esim. sormenjälki). Vahvaa tunnistamista on mahdollista käyttää verkossa kytkemällä kaksivaiheinen tunnistaminen päälle, jolloin käyttäjältä vaaditaan tekstiviestillä saatu kertakäyttöinen koodi, käyttäjätunnus sekä salasana. Salasanat edustavat heikkoa tunnistamista, sillä niissä täyttyy ainoastaan yksi kolmesta ehdosta. (viestintävirasto, 2014) Käyttäjän on vältettävä ennalta-arvattavia salasanoja. Käyttäjän on myös noudatettava hyvää salasanakäytäntöä. Hyvä salasana on vähintään kahdeksan merkkiä pitkä ja sisältää isoja ja pieniä kirjaimia, erikoismerkkejä sekä numeroita. Salasana ei saa olla minkään kielen tunnettu sana. Jokaisessa palvelussa on oltava eri salasana. Salasanoja tulee myös vaihtaa säännöllisesti. (Peltomäki & Norppa, 2015) Peltomäen ja Norpan ohje eroaa melko suuresti viestintäviraston ohjeesta, jossa suositellaan salasanan pituudeksi aina yli 15-merkkiä. Käyttäjän näkökulmasta on aina parempi noudattaa konservatiivisempaa tietoturvaohjeistusta ja valita mieluummin pidempi salasana. Huonoina puolina pidemmässä salasanassa on mahdollisesti vaikeus muistaa se. Hyvänä puolena on kasvanut salasana-avaruus, josta sen arvaaminen vie koneellisestikin liikaa aikaa. Käyttäjä voi suojautua hyvillä salasanakäytännöillä kyberavusteisia identiteettivarkauksia, hakkerointia ja motivaatiorikoksia vastaan. Näitä rikoksia toteuttavat välinpitämättömät, ammattirikolliset, hakkerit ja valtiot. (Peltomäki & Norppa, 2015)

Tärkeimmistä tiedostoista on säännöllisesti otettava varmuuskopiot ja säilytettävä ne turvallisessa paikassa. Varmuuskopioista palautuminen on hyvä testata säännöllisesti, sillä varmuuskopio toimii vasta kun siitä voidaan palautua. (Peltomäki & Norppa, 2015) Varmuuskopiot ovat hyvä varautumistapa tällä hetkellä kasvavaan kiristyshaittaohjelmarikollisuuteen. Kiristyshaittaohjelmaiskussa ainut tapa palautua maksamatta lunnaita on käytännössä aina palautuminen uusimmasta varmuuskopiosta. Jossakin tapauksissa on raportoitu myös

mahdollisuus palautua, mikäli haittaohjelma on kirjoitettu huolimattomasti. Tällaiset tilanteet ovat kuitenkin harvinaisia ja haittaohjelmat tunnistetaan nopeasti virustentorjuntaohjelmissa. (Viestintävirasto, 2016c) Varmuuskopioinnilla suojaudutaan haittaohjelmia ja hakkerointia vastaan. Rikoksia toteuttavat hakkerit, ammattirikolliset ja valtiot. (Peltomäki & Norppa, 2015)

Näyttää siltä, että yksilön osalta tärkein yksittäinen toiminto kyberrikokselta suojautumisessa on tietoturvatietoisuuden kasvattaminen sekä tietoturvaohjelmistojen ajan tasalla pitäminen.

4.2 Organisaatio

Fyysinen turvallisuus tarkoittaa valtionhallinnon vahtiohjeistuksen mukaan henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaamista tuhoja ja vahinkoja vastaan. Fyysinen turvallisuus sisältää mm. kulun-, pääsyn- ja tilojenvalvonnan, vartioinnin, palo-, vesi- ja sähköturvallisuuden sekä murtovahinkojen torjunnan. (Valtiovarainministeriö, 2008) Fyysisen turvallisuuden kannalta on organisaatiossa pohdittava toimitilojen kulunvalvontaa ja pääsyoikeuksia henkilöstöllä ja niitä on syytä rajoittaa niin, että henkilöillä on pääsy ainoastaan niihin tiloihin, joita he tarvitsevat päivittäisessä työssään. Fyysinen turvallisuuden tarkoituksena on pyrkiä poistamaan mahdollinen fyysinen pääsy tärkeätä tietoa varastoiville laitteille, sillä fyysinen pääsy useimmissa tilanteissa mahdollistaa erilaisten tietoverkkoon toteutettujen turvajärjestelmien täydellisen ohittamisen. Tiloissa, joissa käsitellään korkean turvaluokituksen informaatiota, on pohdittava myös tilojen äänieristys sekä mahdollinen sähkömagneettinen hajasäteily. (Andreasson & Koivisto, 2013) Fyysisellä turvallisuudella voidaan varautua kyberavusteisia petoksia ja motivaatiorikoksia vastaan. Näitä rikoksia toteuttavat tietämättömät, välinpitämättömät ja ammattirikolliset. (Peltomäki & Norppa, 2015)

Etä- ja mobiilityöllä tarkoitetaan työtä, joka toteutetaan organisaation oman lähiverkon ulkopuolelta, käyttäen hyväksi resursseja jotka ovat organisaation sisäverkossa (Valtiovarainministeriö, 2008). Etä- ja mobiilityössä on varmistuttava tiedon salauksesta sekä sivullisten mahdollisesta tiedon urkkimisesta, kun työntekijä työskentelee jossakin julkisessa kulkuvälineessä. (Andreasson & Koivisto, 2013) Henkilöstölle on luotava liikkuvan työn politiikka ja koulutettava henkilökunta noudattamaan sitä. Tietoturvaratkaisut on sovellettava kaikkien käyttäjien kaikkiin laitteisiin. Tieto on suojattava levossa sekä liikkeessä. (C.E.S.G., 2012) Tietoverkossa käyttäjän ja organisaation palvelimen välinen liikenne on salattava käyttäen VPN (virtual private network) tekniikkaa. VPN toimii tehokkaana suojana tiedolle ja mahdollistaa käyttäjän saavuttaa yrityksen sisäverkossa olevat resurssit. (Weber, 2015) Etä- ja mobiilityön fyysisellä ja digitaalisella suojauksella suojaudutaan kyberavusteisia identiteettivarkauksia ja petoksia sekä hakkerointia vastaan. Näitä rikoksia toteuttavat tietämättömät, välinpitämättömät, ammattirikolliset sekä valtiot.

Organisaatioon on luotava politiikka, jolla määritellään hyväksyttävät ja turvalliset tavat käyttää organisaation tietoja ja järjestelmiä. Organisaatiossa on otettava käyttöön henkilöstölle koulutusohjelma ja huolehdittava käyttäjien kyberriskien tietotason ylläpidosta. (C.E.S.G., 2012) On arvioitu, että organisaatiossa vallitsevan tietoturvapolitiikan puute, vaikeus tai henkilökunnan ymmärtämättömyys on syynä useampaan kuin yli puoleen tietomurroista. Työntekijät laiminlyövät tietoturvapolitiikan tai jättävät noudattamatta sitä, sillä he eivät välttämättä ymmärrä merkityksiä politiikkojen takana. Työntekijöiden koulutuksessa onkin panostettava ennemmin politiikan rationalisoimiseen kuin rangaistusten kehittämiseen. (Siponen & Vance, 2010) Henkilöstön koulutus ja tietoturvapolitiikka yhdessä vaikuttavat olevan yksittäisistä toimista tärkein ehkäisemään kyberrikoksen toteutumista. (Choo, 2011b) Henkilöstön koulutuksella voidaan ehkäistä petoksia, tietojenkalastelua, haittaohjelma tartuntoja, hakkerointia ja roskapostin leviämistä.

Hätätilanteen hallinta on organisaatiossa oltava tehokasta ja ennalta suunniteltua. Yhteiskunnan turvallisuusstrategiassa määritellään, yhteiskunnan turvallisuuden kannalta, kriittiseksi osaksi tietoliikenteen ja tietojärjestelmien toiminnat. Organisaation kannalta tietoturvan hätätilanteessa organisaatiosta on syytä olla yhteydessä viestintäviraston kyberturvallisuuskeskukseen. Kyberturvallisuuskeskuksen keskeinen tehtävä on valvoa viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta sekä tuottaa valtiolle ja yrityksille tilannekuvaa kybertoimintaympäristöstä (Viestintävirasto, 2017). Organisaatiolta on löydyttävä jatkuvuussuunnitelma sellaisiin uhkiin, joiden seuraukset liiketoiminnalle ovat merkittävät ja todennäköisyys keskitasoa. Tällaisia uhkia ovat tulipalot, vesivahingot, verkkohyökkäykset, erityisen voimakkaat sääilmiöt sekä henkilöriskit. Jatkuvuussuunnitelmassa on otettava kantaa sellaisiin toimenpiteisiin, joiden avulla häiriötilanteesta voidaan palautua häiriöttömälle tasolle. Jatkuvuussuunnitelmassa näitä osioita kutsutaan toipumissuunnitelmaksi ja valmiussuunnitelmiksi. Organisaatiossa on oltava varmoja siitä, että vastuut ja toipumissuunnitelmat poikkeustilanteita varten ovat käytössä ja ne toimivat. Vastuuhenkilöt on koulutettava ja valmius- ja jatkuvuussuunnitelmia on testattava käytännössä. Mahdollisista tietoturvaloukkauksista on raportoitava aina viranomaisille. (C.E.S.G., 2012) Suunnitelmia on myös testattava, sillä mikäli suunnitelma ei ole realistinen, ei siitä ole organisaatiolle hyötyjä. (Andreasson & Koivisto, 2013) Häiriötilanteista toipumisella ja jatkuvuuden suunnittelulla on merkittävä vaikutus liiketoiminnan kannalta. Mahdollisesti lyhyetkin katkokset liiketoiminnan prosessissa saattavat aiheuttaa tuhoisia vaikutuksia, joista toipumiseen saattaa kulua useita kuukausia tai vuosia. Kriittisen infrastruktuurin osalta esimerkiksi sähkön- tai vedentuotannossa ja -siirrossa tapahtuvat häiriöt saattavat olla todella merkittäviä yhteiskunnan kannalta. Hätätilanteiden suunnittelu yleensä toimii tilanteessa, jossa rikos on jo päässyt tapahtumaan. (Andreasson & Koivisto, 2013) Tällaisia tilanteita ovat esimerkiksi palvelunestohyökkäykset. Palvelunestohyökkäyksiä toteuttavat hakkerit, välinpitämättömät, ammattirikolliset, haktivistit ja valtiot.

Tietoturvallisuudelle on toteutettava tietoturvallisuuden hallintasuunnitelma. Suunnitelman tarkoituksena on suunnitella, toteuttaa, noudattaa, seurata, arvioida, ylläpitää sekä kehittää organisaation tietoturvallisuutta. Tietoturvallisuuden standardi ISO27001 mukaan organisaation tulee luoda, toteuttaa, käyttää, valvoa, katselmoida, ylläpitää ja jatkuvasti kehittää dokumentoitua tietoturvallisuuden hallintajärjestelmää, joka tukee organisaation liiketoimintoja ja organisaatioon kohdistuvia riskejä. (Andreasson & Koivisto, 2013) ISO27001 standardi perustuu tilastotieteilijä William Demingin kehittämään PDCA-malliin (International Organization for Standardization, 2016). Malli tulee sanoista plan, do, check ja act. Suomeksi sillä tarkoitetaan suunnittelemista, toteuttamista, arviointia ja toimintaa. Suunnitteluvaiheessa organisaation on määriteltävä tietoturvapolitiikka, -tavoitteet, -päämäärät, -prosessit ja menettelytavat, jotka ovat olennaisia organisaation riskienhallinnalle sekä tietoturvallisuuden kehittämiselle. Toteuttamisvaiheessa toteutetaan suunnitteluvaiheessa tuotettua suunnitelmaa, joka sisältää tietoturvapolitiikan, turvamekanismit, prosessit sekä menettelytavat. Arviointi vaiheessa seurataan ja mitataan soveltuvien osien suorituskykyä ja verrataan tuloksia tietoturvapolitiikan tavoitteisiin ja käytännön kokemukseen. Näistä raportoidaan johdolle, joka tekee tarvittavat päätökset seuraavassa vaiheessa. Toimimisvaiheessa korjataan aikaisemmissa vaiheissa havaitut puutteet ja prosessi aloitetaan uudelleen alusta. Tietoturvallisuuden hallintajärjestelmän prosessi on toteutettava vähintään kerran vuodessa jotta se on tehokas. (Andreasson & Koivisto, 2013) Tietoturvallisuuden hallintasuunnitelmalla pyritään ennaltaehkäisemään rikoksia ennen kuin ne tapahtuvat. Suunnitelmalla voidaan ehkäistä haittaohjelmia, hakkerointia ja palvelunestohyökkäyksiä.

Käyttäjätilien osalta on otettava käyttöön käyttäjätilien hallintaprosessi, jonka perusteella käyttöoikeuksia rajoitetaan sekä monitoroidaan käyttäjien aktiivisuutta. (C.E.S.G., 2012) Organisaatiossa on tärkeää harjoittaa myös niin sanottua vähiten oikeutetun käyttäjän periaatetta. Tällä tarkoitetaan sitä, että käyttäjälle annetaan ainoastaan niin vähän oikeuksia kuin tämä tarvitsee toteuttaakseen työnsä. Tällä pystytään minimoimaan sisäisen hyökkääjän vaikutus organisaatioon. Sisältä päin tuleva hyökkäys saattaa monessa suhteessa olla todella vaikea, sillä sisältä päin tulevassa hyökkäyksessä käyttäjällä on pääsy hänen tuntemaan järjestelmään ja tietoa kriittisestä informaatiosta. Sisäisen uhalla on merkittäviä vaikutuksia, koska sillä saattaa olla tuhoisia vaikutuksia ydintiedon luottamuksellisuuteen, kiistämättömyyteen ja saatavuuteen. (Warkentin & Willison, 2009) Käyttöoikeuksien hallinnassa on otettava myös huomioon mahdolliset alihankkijat, kumppanit sekä konsultit, joille annetaan yrityksessä käyttäjätunnuksia. Nämä käyttöoikeudet tulee poistaa välittömästi, kun toimijan tarve käyttötunnuksille päättyy. (Hyppönen & Tuominen, 2017) Käyttäjätilien hallinnalla ehkäistään kyberavusteisia identiteettivarkauksia, petoksilta, hakkeroinnilta ja motivaatio rikoksilta.

Tietoverkko on suojattava ulkoisilta ja sisäisiltä uhilta. Verkon turvallisuudessa on huomioitava myös rajapinnat. Organisaation on suodatettava palomuurisäännöillä pääsyä järjestelmään sekä vahingollisen sisällön hakemista. Palomuureja on sijoitettava tietoverkkoon useita ja niillä on pyrittävä segmentoimaan

tietoverkkoa. Palomuurisääntöjen osalta on huomioitava niiden tarkastamisen aikaväli, sillä palomuurisääntöjen muuttaminen on organisaatiossa usein arkipäiväistä. Organisaatiossa on varmistettava, että tietojärjestelmät ovat konfiguroitu turvallisesti ja ne noudattavat yleisesti hyviä käytäntöjä. (C.E.S.G., 2012) Turvallinen suunnittelu lähtee tietoverkkojen ja tietojärjestelmien topologian määrittelystä. Tietoturvallisuus on otettava huomioon suunnitteluvaiheessa, sillä silloin järjestelmille ja tietoverkoille on helpompi tehdä muutoksia. Jälkikäteen tehdyt muutokset aiheuttavat usein katkoksia liiketoiminnalle. Tietoverkkojen suunnittelussa on tiedettävä mitä laitteita verkkoon kytketään ja minkälaista tietoa niissä siirretään. Tietoverkon toteuttamisessa on huomioitava dokumentaatio ja sen ajan tasalla pitämisestä on pidettävä huolta. Dokumentaatio on toteutettava erikseen OSI-mallin alemmilla kerroksilla (fyysinen-, data-, verkko- ja kuljetuskerros) sekä ylemmillä kerroksilla (istunto-, esitystapa- ja sovelluskerros), jotta pystytään paikantamaan mahdollisessa vika-/hyökkäystilanteessa tehokkaasti ongelmakohta ja sulkemaan se ulos verkosta. (Andreasson & Koivisto, 2013) Mahdollisesti ulkopuolelle verkkoon näkyvät palvelimet on sijoitettava verkon topologiassa ns. eteisverkkoon, eli verkossa sellaiseen kohtaan, josta ei ole pääsyä kriittisiin järjestelmiin (Valtiovarainministeriö, 2008). Verkon segmentoinnilla suojaudutaan hakkerointia ja palvelunestohyökkäyksiä vastaan.

Tietoverkossa pyritään levittämään haittaohjelmia. Haittaohjelmia levitetään sosiaalisessa mediassa, sähköpostin liitetiedostoina sekä siirrettävissä tiedonsiirtovälineissä. Haittaohjelmia on pystytty siirtämään kohdennettuina hyökkäyksinä myös sellaisiin tiloihin, jotka ovat irti verkosta (Farwell & Rohozinski, 2011). Työasemissa on oltava asennettuna haittaohjelmien varalta virustentorjuntaohjelmistot, mutta käyttäjiä on kuitenkin jatkuvasti koulutettava huomioimaan erilaiset hyökkäykset, sillä edes virustentorjunta yhdistettynä palomuuriin ei pysty luomaan täydellistä suojaa, koska virustentorjuntaohjelmistot perustuvat aina tunnettuihin tunnisteisiin jo havaituista haittaohjelmista. (Andreasson & Koivisto, 2013) Henkilöstöllä on oltava sekä riittävä ohjeistus että toimiva virustorjuntajärjestelmä, jotka ovat sopivia ja niitä voidaan käyttää kaikilla liiketoiminta-alueilla. (C.E.S.G., 2012) Käyttäjien koulutus ja tietoturvatietoisuuden lisääminen yhdistettynä ajantasaisiin ohjelmistoihin sekä tietoturvapolitiikkaan on tehokkain ehkäisy haittaohjelmia vastaan. Samoilla toimilla voidaan ehkäistä myös hakkerointia sekä palvelunestohyökkäyksiä.

Organisaatiossa on otettava käyttöön seurantastrategia sekä -käytännöt. Näillä seurataan kaikkia informaatioteknologiajärjestelmien ja verkkojen liikennettä sekä pyritään löytämään niistä poikkeamia jotka viittaavat hyökkäykseen. (C.E.S.G., 2012) Seurantaa voidaan toteuttaa jälkikäteen lokijärjestelmällä ja reaaliaikaisesti tietoverkon tunkeutumisenesto- ja havainnointijärjestelmillä. Lokijärjestelmillä tarkoitetaan järjestelmää, joka kerää tapahtumat aika- ja asiajärjestykseen. Lokijärjestelmän perusteella voidaan tutkia ja analysoida jo tapahtuneita muutoksia tietojärjestelmässä. Lokijärjestelmä tuottaa tärkeää tietoa mm. rikoksen tutkinnassa ja myöhemmin näyttöä rikoksesta tuomioistuimelle. Lokitiedostoja voidaan käyttää myös mahdollisissa vikatilanteissa, kun pyritään saamaan

järjestelmä takaisin toimintaan sekä välttämään sama virhetilanne tulevaisuudessa. Lokit on hyvä jakaa neljään eri kategoriaan. Käyttöloki, johon kirjautuu tietojärjestelmän käyttöön liittyvät asiat. Muutosloki, johon kirjautuu tietojärjestelmän tietoihin tehdyt muutokset ja kuka nämä muutokset on tehnyt. Luovutusloki, johon kirjautuu aina tilanteet, joissa tietoa luovutetaan organisaatiosta ulos. Virheloki, johon kirjautuu aina kun tietojärjestelmässä havaitaan virhe tai muu merkittävä tekninen tapahtuma. (Andreasson & Koivisto, 2013) Lokitiedostojen ylläpito on tärkeätä myös tiedonhallinnan takia, sillä tietoa liikkuu verkossa sekä fyysisillä laitteilla ulos organisaatiosta jatkuvasti. Suomessa viranomaiset noudattavat sekä ohjeistavat organisaatioita toimimaan samalla tavalla, tosin nimikäytännöt ovat osaltaan erilaiset mm. luovutuslokista puhutaan haltialokina (Viestintävirasto, 2016a). Jopa 40% tapauksissa organisaatiosta varastettu tieto liikkui fyysisessä medialla, kuten muistitikulla ulos organisaatiosta (McAfee Labs, 2016). Seurantastrategialla voidaan ehkäistä motivaatiorikoksia sekä hakkerointia. Seurantastrategialla voidaan huomata palvelunestohyökkäykset, mutta niiden estäminen ei passiivisella seuraamisella ole mahdollista. (Zargar, Joshi, & Tipper, 2013)

Taulukossa 6 esitellään yksilön ja organisaation suojautuminen kyberrikollisuutta vastaan. Taulukossa on yhdistettynä aiemmin esitellyt kyberavusteiset rikokset ja kyberriippuvaiset rikokset. Yksilön suojautuminen perustuu sisältöluvun 4.1 havaintoihin, jotka hyödyntävät useita lähteitä. Organisaation suojautuminen perustuu sisältöluvun 4.2 havaintoihin, jotka hyödyntävät myös useita eri lähteitä. Taulukosta on luettavissa suojautumismahdollisuudet yleisesti kyberavusteisia ja kyberriippuvaisia vastaan sekä yksittäistä kyberavusteista ja kyberriippuvaista rikosta vastaan. Taulukko on itse laadittu tutkielmassa esiteltyjen lähteiden perusteella.

TAULUKKO 6 Yksilön ja organisaation kyberrikokselta suojautuminen

	Rikos / uhka	Yksilön suojautuminen rikosta vastaan	Organisaation suojautuminen rikosta vastaan
Kyberavusteiset rikokset	**Kyberavusteinen petos**	Tietoturvatietoisuus	Fyysinen turvallisuus, tietoturvapolitiikka, käyttöoikeuksien hallinta, etäyhteyksien salaaminen ja henkilöstön koulutus
	Kyberavusteinen tietojenkalastelu	Tietoturvatietoisuus	Henkilöstön koulutus
	Kyberavusteinen identiteettivarkaus	Tietoturvatietoisuus, vahvat salasanat ja mobiililaitteiden suojaaminen	Käyttöoikeuksien hallinta ja etäyhteyksien salaaminen
Kyberriippuvaiset rikokset	**Haittaohjelmat**	Varmuuskopiointi, tietoturvatietoisuus, työasemienpäivitys ja tietoturvaohjelmistot mobiililaitteissa sekä työasemassa	Tietoturvallisuuden hallintasuunnitelma, henkilöstön koulutus, varmuuskopiointi, työasemien päivitys ja tietoturvaohjelmistot
	Hakkerointi	Varmuuskopiointi, tietoturvatietoisuus vahvat salasanat, työasemienpäivitys ja tietoturvaohjelmistot	Hallintasuunnitelma, henkilöstön koulutus, seurantastrategia, käyttöoikeuksien hallinta, etäyhteyksien salaaminen ja verkon segmentointi
	Palvelunestohyökkäykset	*(ei käytännössä mahdollisuutta suojautua)*	Hätätilanteiden-, tietoturvallisuuden hallintasuunnitelmat ja verkon segmentointi
	Roskapostin levittäminen	Tietoturvatietoisuus, työasemienpäivitys ja tietoturvaohjelmistot	Henkilöstön koulutus, Työasemien päivitys ja tietoturvaohjelmistot
	Bottiverkot	Tietoturvatietoisuus, työasemienpäivitys ja tietoturvaohjelmistot	Työasemien päivitys ja tietoturvaohjelmistot
	Motivaatiorikokset	Tietoturvatietoisuus, vahvat salasanat ja mobiililaitteiden suojaaminen	Fyysinen turvallisuus, käyttöoikeuksien hallinta ja seurantastrategia

5 YHTEENVETO

Kyberrikollisuutta ilmenee nykyisin kaikissa verkottuneissa tietoyhteiskunnissa. Tietoverkkorikokset ilmenevät haittaohjelmina, tietomurtoina, tietokoneavusteisinapetoksina sekä erilaisina huijauksina. Kyberrikosten uhriksi joutuvat sekä yksityishenkilöt, että organisaatiota. (Peltomäki & Norppa, 2015) Kyberrikoksen uhriksi joutuminen on nykyisin todennäköisempää kuin tavanomaisen rikoksen uhriksi joutuminen. (Hintsala, 2016). Tätä tukee myös Symantecin (2011) teettämä tutkimus, jossa kyberrikoksen uhriksi joutumisen todennäköisyydeksi on arvioitu 1/2.27. Rikollisuus on seurannut verkkoon luonnollisena jatkumona, sillä kuluttaminen, kaupankäynti ja palvelut ovat siirtyneet verkkoon. Sotateorian tohtori Martti Lehto kuvailee verkossa tehtailtavien rikosten olevan kustannustehokasta, sillä kiinnijäämisen riski on pieni, rangaistukset ovat alhaisia tai lainsäädäntö ei kyseisessä maassa tunne rikosta. (Peltomäki & Norppa, 2015, s. 34).

Kyberrikollisuutta esiintyy verkossa kyberavusteisina rikoksina sekä kyberriippuvaisina rikoksina. Kyberavusteiset rikokset ovat perinteisiä rikoksia, joita toteutetaan tietokoneiden ja tietoverkkojen avulla. Tällaisia rikoksia ovat mm. sähköisillä kauppapaikoilla tapahtuvat petokset, kyberavusteinen tietojenkalastelu sekä kyberavusteinen identiteettivarkaus. Kyberavusteisissa rikoksissa tietoverkko toimii rajapintana rikokselle, mutta itse rikos ei edellytä tietotekniikkaa. Kyberriippuvaiset rikokset ovat rikoksia joiden toteuttaminen vaati tietokoneita ja/tai tietojärjestelmiä rikoksen tekovälineenä. Kyberriippuvaisia rikoksia ovat mm. tietomurrot ja palvelunestohyökkäykset. (Viestintävirasto, 2017) Kyberrikoksia tehtailevat kolmeen pääluokkaan ja kuuteen alaluokkaan kategorisoidut rikolliset. Pääluokassa ovat rikolliset, haktivistit ja valtiot. Taylor (2005), Hyppönen (2012) sekä Peltomäki ja Norppa (2015) kaikki käyttävät kyberrikollistensa luokittelussa näitä kolmea ryhmää. Taylor (2005) sekä Peltomäki ja Norppa (2015) jakavat rikolliset vielä neljään eri alaluokkaan, jotka ovat tietämättömät, välinpitämättömät, hakkerit sekä ammattirikolliset. Hyppönen (2012) puhuu osittain samasta luokittelusta, mutta ei kuitenkaan ota kantaa rikollisten sisällä oleviin eri ryhmiin Näillä ryhmittymillä on jokaisella erilaisia motiiveja sekä tapoja hyötyä rikoksesta. Haktivistit pyrkivät saavuttamaan mahdollisimman laajaa huomiota ajamalleen ideologiselle, poliittiselle tai uskonnolliselle agendalle. Haktivistit käyttävät toiminnassaan palvelunestohyökkäyksiä, virtuaalisia istumalakkoja sekä verkkosivujen tärvelemisiä. He eivät varsinaisesti hae rahallista hyötyä, vaikkakin toisinaan heidän taloudellinen toimintatapa on aiheuttaa tappioita toiminnan kohteena olevalle toimijalle. Välinpitämättömät ovat rikoksen tekijöitä, jotka eivät välttämättä miellä rikostaan rikokseksi vaan toimivat mielestään harmaalla alueella. Välinpitämättömät toteuttavat vähäisiä tietomurtoja, kiusantekoa sekä jakavat tekijänoikeuksien alaista materiaalia verkossa. Välinpitämättömät pyrkivät saavuttamaan toimillaan hupia, vähäistä taloudellista hyötyä sekä saamaan muuten verkossa maksullista sisältöä ilmaiseksi. Tietämät-

tömät ovat rikoksentekijöitä, jotka eivät välttämättä itse tiedä osallistuvansa rikokseen ja siksi toimivat hyvässä uskossa. Tietämättömät pyrkivät saavuttamaan rahallista tai rahaan verrattava etuutta. Tietämättömillä on myös kohonnut riski joutua itse rikoksen uhriksi, sillä he toimivat hyvässä uskossa ja ovat helposti huijattavissa. Hakkereilla tarkoitetaan tietoteknisesti edistyneitä henkilöitä, joiden toiminta ilmene identiteettivarkauksina, tietomurtoina, palvelunestohyökkäyksinä, haittaohjelmina sekä näiden myymisenä tuotteina tai palveluina ammattirikollisille. Hakkereiden motiivina on näyttämisen halu, taloudellinen hyötyminen sekä maineen ja kunnian saavuttaminen. Hakkerit tuottavat ammattirikollisille tarvittavia resursseja tietoverkkorikollisuuteen. Näitä resursseja ovat käyttäjätiedot, bottiverkot, yritysvakoiluilla saavutetut tiedot, haittaohjelmat sekä muut rikollisille tarjottavat palvelut. Valtioiden osalta tietoverkkorikollisuus näkyy yhteiskunnassa vähäisesti, sillä valtioilla on suuret resurssit ja yleensä on epäselvää, mikä valtio kyberiskuja on toteuttanut. Yleensä vaikutukset tulevat esille vasta huomattavasti myöhemmin (Langner, 2011). Valtioiden osalta motiivina ovat tiedustelutiedon saavuttaminen, taktisten kyberaseiden kehittäminen sekä strategisen ja kansallisen edun saavuttaminen.

Yksilön ja organisaation on suojauduttava kyberrikollisuutta vastaan, sillä riski joutua rikoksen uhriksi on merkittävä. Kyberrikosten määrä tulee tulevien vuosien aikana kasvamaan merkittävästi (Choo, 2011b). Kyberrikollisuudelta suojautumiseen yksilön ja organisaation osalta tärkein yksittäinen toimi näyttää olevan yksilöjen tietoisuuden lisääminen koulutuksen kautta. Valtaosa rikoksista vaatii onnistuakseen ihmisen tekemään jonkin kriittisen päätöksen, jotta hyökkäys onnistuu. Yksilön sekä organisaation on myös panostettava ajantasaisiin käyttöjärjestelmä päivityksiin sekä tietoturvaohjelmistoihin. Yksilön ja organisaation osalta on pidettävä huolta hyvästä tietoturvapolitiikasta, johon kuuluvat vahvat salasanat, sähköpostiin liittyvät politiikat sekä hätätilanteiden varalle suunniteltu prosessi. Organisaation osalta on panostettava verkon segmentointiin, jatkuvuussuunnitteluun sekä käyttäjätilien hallintaan. (Andreasson & Koivisto, 2013) Organisaation on seurattava sisäverkossa sekä järjestelmissä tapahtuvia muutoksia ja ne on kirjattava ylös myöhempää tarkastelua ja tutkintaa varten. (Viestintävirasto, 2016a)

Kyberrikollisuus tulee kasvamaan ilmiönä tulevaisuudessa. (Hyppönen & Tuominen, 2017) Tulevaisuudessa pelottavia näkökulmia tuovat aiheet kyberterrorismista. Tällä hetkellä vielä ensimmäistäkään aidosti merkittävää kyberterrori-iskua ei ole vielä tavattu ja sen riskiä ei pidetä yleisesti merkittävänä. Kuitenkin perinteisesti terrorismin vastaisessa työssä edelläkävijänä tunnettu Yhdysvallat tekee miehittämättömillä ilma-aluksilla iskuja, joiden kohteen on ISIS:n hakkerit ja tietojärjestelmä osaajat. (Kumar, 2016) Tällainen kehitys viittaa siihen, että ainakin Yhdysvallat ovat huolissaan kyberterrorismista, joka antaisi viitteitä myös siihen, että muiden valtioiden tulisi myös olla huolissaan sen mahdollisista vaikutuksista. Kyberterrorismi on tuore ja toistaiseksi epäselvä aihe. Jatkotutkimuksena voitaisiin tutkia kyberterrorismia ja kyberterroristien mahdollisia toimintatapoja. Kyberterrorismin merkitys tulee nousemaan ja mahdollisen kyberterrori-iskun mahdollisuus tulee kasvamaan. (Wilson, 2008)

LÄHTEET

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., Nunamaker, J. F., & Abbasi Sheldon, A. B. (2010). Detecting Fake Websites: The Contribution of Statistical Learning Theory Detecting Fake Websites. *MIS Quarterly, 3423403(19)*, 435–461.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265-300). Springer Berlin Heidelberg.

Andreasson, A., & Koivisto, J. (2013). Tietoturvaa toteuttamassa. Tietosanoma.

Backhouse, J., & Dhillon, G. (1996). Structures of responsibility and security of information systems. *European Journal of Information System, 5*, 2–9.

Beal, V. (2004). The Difference Between a Virus, Worm and Trojan Horse - Webopedia. Haettu 16.12.2016 osoitteesta http://www.webopedia.com/DidYouKnow/Internet/virus.asp

Brown, C. (2015). White or Black Hat, An Economic Analysis of Computer Hacking White or Black Hat, An Economic Analysis of Computer Hacking, 0–26.

C.E.S.G. (2012). 10 Steps To Cyber Security, 20. Haettu 29.12.2016 osoitteesta https://www.cyberessentials.org/system/resources/W1siZiIsIjIwMTQvMDYvMDQvMTdfNDdfMTdfNjMwXzEwX3N0ZXBzX3RvX2N5YmVyX3NlY3VyaXR5LnBkZiJdXQ/10-steps-to-cyber-security.pdf

Candolin, C. (2012). Akateeminen upseerikoulutus. Kylkirauta, 1, 6. Haettu 20.1.2017 osoitteesta http://www.kylkirauta.fi/images/pdf/10/kr1_12.pdf

Chang, R. K. C. (2002). Defending against flooding-based distributed denial-of-service attacks: A tutorial. *IEEE Communications Magazine, 40(10*), 42–51.

Choo, K. K. R. (2011a). Cyber threat landscape faced by financial and insurance industry. *Trends and Issues in Crime and Criminal Justice, (408).*

Choo, K. K. R. (2011b). The cyber threat landscape: Challenges and future research directions. *Computers and Security, 30(8),* 719–731.

Christodorescu, M., Jha, S., Seshia, S. A., Song, D., & Bryant, R. E. (2005). Semantics-aware malware detection. 2005 *Ieee Symposium on Security and Privacy, Proceedings*, 32–46.

Das, S. (2000). The Availability of the Fair Use Defense in Music Piracy and Internet Technology. *Federal Communications Law Journal, 52(3).*

Durcekova, V., Schwartz, L., & Shahmehri, N. (2012). Sophisticated Denial of Service Attacks Aimed at Application Layer, 55–60.

Faraj, S. & Sambamurthy, V. (2006). Leadership of Information Systems Development Projects. *IEEE Transactions on Engineering Management, 53*(2), 238–249.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. Survival, 53(1), 23–40.

Felson, M., & Clarke, R. V. (1998). Opportunity Makes the Thief Practical theory for crime prevention.

Furnell, S., Bryant, P., & Phippen, A. (2007). Assessing the security perceptions of personal Internet users.

Goucher, W. (2010). Being a cybercrime victim. *Computer Fraud & Security, 2010(10),* 16–18.

Hagan, F. E. (2010). Crime Types and Criminals. SAGE Publications. Haettu 10.2.2017 osoitteesta https://books.google.fi/books?id=UNKFHlXIaycC

Hampson, N. C. N. (2012). Hacktivism: A New Breed of Protest in a Networked World. *Boston College International and Comparative Law Review* (Vol. 35).

Helfenstein, S., & Saariluoma, P. (2014). How cyber breeds crime and criminals. In V. Snasel (Ed.), DigitalSec 2014 Proceedings: The International Conference on Digital Security and Forensics (pp. 76-90). Wilmington: The Society of Digital Information and Wireless Communications (SDIWC).

Hintsala, J. (2016). Verkossa rikoksen uhriksi joutuminen on todennäköisempää kuin kadulla | Yle Uutiset | yle.fi. Haettu 26.12.2016 osoitteesta http://yle.fi/uutiset/3-8859957

Hoffman, L. J., Rosenberg, T., & Washington, G. (2005). Types of cyberexercises. *IEEE Security & Privacy 3.5,* 27–33.

Hyppönen, M. (2012). The three types of online attackers - TechRepublic. Haettu 19.2.2017 osoitteesta http://www.techrepublic.com/blog/it-security/the-three-types-of-online-attackers/

Hyppönen, M., & Tuominen, T. (2017). State of cyber security. Haettu 20.2.2017 osoitteesta https://www.f-secure.com/documents/996508/1030743/cyber-security-report-2017

International Organization for Standardization. (2016). ISO/IEC 27001 - Information security management. Haettu 19.2.2017 osoitteesta http://www.iso.org/iso/iso27001

Jewkes, Y., & Yar, M. (2013). Handbook of Internet Crime. Taylor & Francis. Haettu 20.12.2016 osoitteesta https://books.google.fi/books?id=1WyglzwkN-QC

Joseph, A. E. (2006). Cybercrime definition. Haettu 1.1.2017 osoitteesta http://www.crime-research.org/articles/joseph06/

Kirwan, G., & Power, A. (2011). The Psychology of Cyber Crime), 55–57. https://doi.org/10.4018/978-1-61350-350-8

Kovacich, G. L. (1999). Hackers: Freedom Fighters of the 21Sf Century. *Computers & Security, 18,* 573–576.

Kritzinger, E., & Von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers and Security*, 29(8), 840–847.

Kumar, M. (2016). Another ISIS Hacker Killed by U.S Drone Strike in Syria. Haettu 19.2.2017 osoitteesta http://thehackernews.com/2016/01/isis-hacker-drone-strike.html

Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security Privacy, 9(3),* 49–51. https://doi.org/10.1109/MSP.2011.67

Limnéll, J., Majewski, K., & Salminen, M. (2014). Kyberturvallisuus. Jyväskylä: Docendo.

Lindford, S. (2016). Over 90% of email is spam, says Spamhaus founder. Haettu 31.12.2016 osoitteesta http://www.out-law.com/en/articles/2006/september/over-90-of-email-is-spam-says-spamhaus-founder/

Jahankhani, H., & Al-Nemrat, A. (2010). Examination of cyber-criminal behaviour. *International Journal of Information Science and Management, 2010*, 41-48.

McAfee. (2014). Economic impact of cybercrime II. Haettu 2.3.2017 osoitteesta https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

McAfee Labs. (2016). McAfee Labs Threats Predictions Report, (March), 34–35. Haettu 26.12.2016 osoitteesta https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf

McCusker, A. (2006). Transnational organised cyber crime: distinguishing threat from reality. *Crime, Law and Social Change, 46*.

McGuire, M., & Dowling, S. (2013). Cyber crime : A review of the evidence Research of key findings and implications. Haettu 20.01.2017 osoitteesta https://www.gov.uk/government/uploads/.../246751/horr75-chap1

Moir, R. (2013). Defining Malware. Haettu 26.12.2016 osoitteesta https://technet.microsoft.com/fi-fi/en- us/library/dd632948.aspx

Nelms, C. (1999). Internet E-mail Risks and Concerns. *Computers & Security, 18,* 409–418.

Nguyen, D. (2015). State Sponsored Cyber Hacking and Espionage. Haettu 20.12.2016 osoitteesta http://www.infosecwriters.com/Papers/DNguyen_State_Sponsored_CyberHacking_and_Espionage.pdf

Nykodym, N., Taylor, R., & Vilela, J. (2005). PROFILING OF CYBER CRIME Criminal profiling and insider cyber crime. *Digital Investigation, 2(4),* 261-267.

Oikeusministeriö. (2015). Rikoslaki 39/1889 - Ajantasainen lainsäädäntö - FINLEX. Haettu 20.12.2016 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Olin, B. (2014). Tietoturvavinkkejä matkapuhelimen turvalliseen käyttöön. Haettu 20.1.2017 osoitteesta https://www.viestintavirasto.fi/attachments/cert/certtiedostot/Tietoturvavinkkeja_matkapuhelimen_turvalliseen_kayttoon.pdf

Peltomäki, J., & Norppa, K. (2015). Rikos meni verkkoon : näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen. Helsinki: Talentum.

Poliisi. (2016). Poliisi - Kyberrikollisuus. Haettu 26.12.2016 osoitteesta https://www.poliisi.fi/rikokset/kyberrikollisuus

Pounder, C. (2002). Security policy update. *Computers & Security, 21(7),* 620–623.

Salmi, V. (2012). Oikeuspoliittisen Tutkimuslaitoksen. Haettu 20.12.2016 osoitteesta https://helda.helsinki.fi/bitstream/handle/10138/152500/tta_113_Salmi.pdf?sequence=1

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations1. *MIS Quarterly, 34(3),* 487–502.

Symantec. (2011). CYBERCRIME REPORT 2011. *World, 1(650),* 94043.

Taylor, K. (2005). The unusual suspects. Cyber Threats, Methods and Motivations, 18(2), 50–57.

Taylor, P., Jordan, T., & Samuel, A. (2004). Hacktivism and Cyberwars: Rebels with a cause? *Journal of Chemical Information and Modeling (Vol. 53).*

The Federal Bureau of Investigation; (2016). Cyber Crime — FBI. Haettu 1.1.2017 https://www.fbi.gov/investigate/cyber

Thomas, K. (2016). Nine of the worst botnets ever seen. Haetti 31.12.2016 osoitteesta http://www.welivesecurity.com/2015/02/25/nine-bad-botnets-damage/

Valtioneuvoston kanslia. (2010). Yhteiskunnan turvallisuusstrategia. Haettu 20.1.2017 osoitteesta http://www.yhteiskunnanturvallisuus.fi/fi/materiaalit

Valtiovarainministeriö. (2008). Valtionhallinnon tietoturva sanasto. Haettu 20.1.2017 osoitteesta https://www.vahtiohje.fi/c/document_library/get_file?uuid=7e2220f1-cc93-4ba6-8c70-a67869c526cc&groupId=10229

viestintävirasto. (2003). 3/2003 Roskapostituksen aiheuttamat ongelmat. Haettu 20.1.2017 osoitteesta https://www.viestintavirasto.fi/ohjausjavalvonta/ohjeetjajulkaisut/ohjeidentulkintojensuositustenjaselvitystenasiakirjat/32003roskapostituksenaiheuttamatongelmat.html

viestintävirasto. (2014). Salasanat haltuun, Neuvoja salasanojen käyttöön ja hallintaa. Haettu 20.1.2017 osoitteesta https://www.viestintavirasto.fi/attachments/tietoturva/Salasanat_haltuun.pdf

viestintävirasto. (2015). Viestintävirasto - Palveluista säädetään tietoyhteiskuntakaaressa. Haettu 20.1.2017 osoitteesta https://www.viestintavirasto.fi/kyberturvallisuus/palveluidenturvallinenkaytto/palveluntarjoajanyhteystiedot.html

Viestintävirasto. (2010). Ohje tietoturvaloukkaustilanteisiin varautumisesta. Haettu 20.1.2017 osoitteesta http://www.ficora.fi/attachments/suomiry/5jR9D3dp3/Viestintavirasto47C2009M.pdf

Viestintävirasto. (2016a). Lokien keräys ja käyttö, Ohje lokitietojen tallentamiseen ja hyödyntämiseen. Haettu 22.1.2017 osoitteesta https://www.viestintavirasto.fi/attachments/tietoturva/Lokitusohje.pdf

Viestintävirasto. (2016b). Näin meitä_huijataan. Haettu 25.1.2017 osoitteesta https://www.viestintavirasto.fi/attachments/cert/certtiedostot/Nain_meita_huijataan.pdf

Viestintävirasto. (2016c). Selviytymisopas kiristyshaittaohjelmia vastaan. Haettu 26.1.2017 osoitteesta https://www.viestintavirasto.fi/attachments/tietoturva/Kiristyshaittaohjelmat__teemakooste_07_2016.pdf

Viestintävirasto. (2016d). Viestintävirasto - Palvelunestohyökkäykset ovat internetin arkipäivää. Haettu 31.12.2016 osoitteesta https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/04/ttn201604291231.html

Viestintävirasto. (2016e). Viestintävirasto -Tietoverkkorikollisuus - rikoksia verkossa tai verkon avulla. Haettu 26.11.2016 https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/05/ttn201506031327.html

Viestintävirasto. (2017). Viestintävirasto - Kyberturvallisuus. Haettu 17.2.2017 osoitteesta https://www.viestintavirasto.fi/kyberturvallisuus.html

Vorakulpipat, C., Visoottiviseth, V., & Siwamogsatham, S. (2012). Polite sender: A resource-saving spam email countermeasure based on sender responsibilities and recipient justifications. *Computers & Security, 31,* 286–298.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, 18,* 101–105.

Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law and Security Review, 31(5),* 618–627.

Webster, S. C. (2012). Anonymous vows to "destroy" Westboro Baptist Church over Sandy Hook picket plans. Haettu 18.2.2017 osoitteesta http://www.rawstory.com/2012/12/anonymous-vows-to-destroy-westboro-baptist-church-over-sandy-hook-picket-plans/

Wilson, C. (2008). Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE.

Wueest, C. (2014). The continued rise of DDoS attacks, 1–31. Haettu 31.12.2016 osoitteesta http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-continued-rise-of-ddos-attacks.pdf

Wueest, C. (2016). Financial threats 2015. *Security Response, 1.0(March 22),* 30.

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks. *IEEE Communications Surveys and Tutorials, 15(4),* 2046–2069.

Liite 1. Kyberrikoksista tehdyt rikosilmoitukset vuosilta 2000 – 2016